IT341P
Web Security and Ethics
[Onsite]

Course Description:

This course examines the ethical responsibilities in maintaining a Web or intranet/Internet site and the potential chances of misuse. Information access and security issues in managing a Web site are also included.

Prerequisite(s) and/or Corequisite(s):

Prerequisites: IT300P Web Server Administration

Credit hours: 4

Contact hours: 66 (46 Theory Hours, 20 Lab Hours)

SYLLABUS: Web Security and Ethics

Instructor: _____

Office hours: _____

Class hours: _____

MAJOR INSTRUCTIONAL AREAS

Unit 1:

Introduction to Cybercrime

- Define cybercrime
- Identify various common types of cybercrime
- Understand what makes something a cybercrime

Introduction to Ethics

- Define ethics
- Identify common ethical theories
- Understand ethics as it relates to the Web

Unit 2:

Ethics and Web Communication

- Netiquette principles related to communication in cyberspace
- Ethical issues related to free speech and dissemination of hate mail, chain letters, and pornographic literature in cyberspace
- Code of ethics governing communication on the Web

Unit 3:

Ethics and Cyber Content

- Define intellectual property
- Appropriate and inappropriate content available on the Web

- Ethical issues related to intellectual property infringement in cyberspace
- Code of ethics governing the publication and use of cyber content
- Legal aspects of copyright and other intellectual property violations in cyberspace

Unit 4:

Ethics and Privacy in Cyberspace

- Ethical aspects of the right to privacy in cyberspace
- Privacy infringement in cyberspace
- Code of ethics governing the conduct of Internet Service Providers and users
- Legal aspects of privacy infringement in cyberspace

Encryption

- Define encryption
- History of encryption
- Modern methods of encryption
- Using encryption to ensure privacy

Unit 5:

E-Commerce Business Models and Concepts

- Ethical issues involved in online commercial transactions
- Should Web bugs be regulated?
- Types of online commercial transactions and business models
- Security risks in E-commerce transactions
- Key business concepts & strategies applicable to E-commerce

Unit 6:

Security and Encryption

- Secure online transactions
- Using hackers to fight hackers
- Case Study: VeriSign, “The Web’s security blanket”

E-Commerce Payment Systems

- PayPal

- Rocketcash
- Payments over wireless systems
- Case Study: CheckFree

Unit 7:

Malicious Code

- Different types of malicious code
- How malicious code evolves
- Preventing virus attacks
- Restoring the system after a virus attack

Unit 8:

Preventing Web Intrusions

- Threat from intruders
- Methods of intrusion
- Causes of intruder attacks
- Types of intrusion
- Different mechanisms to control intrusion

Unit 9:

Implementing Web Site Security

- Need for Web site security
- Role of Web servers in ensuring Web site security
- Need for securing operating systems
- Areas of security management
- Functioning of IIS
- Security loopholes in IIS and measures to counter them
- Functioning of the Apache Web server
- Security loopholes in the Apache Web server and measures to counter them

Unit 10:

Future Trends in Web Security

The students will use the ITT Tech Virtual Library and the Internet to research new security trends and issues including, but not limited to, the following:

- Need for security management
- Role of QA in security management
- Risks involved in outsourcing
- Security risks to wireless technology

The students will present these topics for informal discussion during class.

COURSE OBJECTIVES

After successful completion of this course, the student will have the opportunity to:

1. Identify cybercrime and understand various common cybercrimes.
2. Identify various types of ethical models.
3. Identify ethical and legal issues involved in different forms of communication over the Web, as well as the operation of networks.
4. Identify ethical and legal aspects of publishing, distributing, and accessing information over the Web; including copyright, trademark, and other intellectual property issues.
5. Identify ethical and legal aspects of an individual's right to privacy in cyberspace.
6. Identify ethical and legal issues related to online commercial transactions.
7. Identify security risks involved in the following areas and the ways to mitigate these risks:
   a. Data security
   b. Privacy
   c. Authentication
8. Identify methods to prevent spread of malicious code.
9. Identify methods to prevent intrusion attacks.
10. Identify methods to ensure Web and network security.
11. Identify legal and technical issues related to Web and network security.

Related SCANS Objectives

1. Acquire and evaluate information.
2. Know the need for a code of ethics for the World Wide Web.
3. Demonstrate competence in ensuring Web site security.
4. Demonstrate competence in preventing the spread of malicious code.
5. Acquire knowledge on how the Web functions.
6. Apply and adapt new knowledge and skills in both familiar and changing situations.

TEACHING STRATEGIES

The curriculum is designed to promote a variety of teaching strategies that support the outcomes described in the course objectives and that foster higher cognitive skills. Delivery makes use of various media and delivery tools in the classroom.

COURSE RESOURCES

Student Textbook

- Quinn, Laudon & Easttom: *Web Security & Ethics*. USA: Pearson Custom Publishing, 2006.
    - **Part 1:** Easttom, Chuck. *Computer Security Fundamentals. New Jersey: Pearson Prentice Hall, 2006.*
    - **Part 2:** Quinn, Michael J. *Ethics for the Information Age. USA: Addison-Wesley, 2006.*
    - **Part 3:** Laudon, Kenneth C. and Carol Guercio Traver. *E-Commerce: Business, Technology, Society. USA: Addison Wesley, 2006.*
    - **Electronic Chapter (for Unit 6):** Chapter 5 from Quinn, Michael J. *Ethics for the Information Age. USA: Addison-Wesley, 2006, can be downloaded from the ITT Virtual Library.*

References and Resources

ITT Tech Virtual Library

Login to the ITT Tech Virtual Library (http://www.library.itt-tech.edu/) to access online books, journals, and other reference resources selected to support ITT Tech curricula.

- Books
    - Pastore, Mike and Emmett Dulaney. *Security+ Study Guide*
    - Tittel, Ed, James Michael Stewart and Mike Chapple. *CISSP: Certified Information Systems Security Professional Study Guide, Second Edition.*
- Other Resources
    - http://www.informIT.com
    - http://www.crimetime.com
    - http://www.astalavista.com

All links to Web references outside of the ITT Tech Virtual Library are always subject to change without prior notice.

EVALUATION & GRADING

COURSE REQUIREMENTS

1. **Attendance and Participation**

   Regular attendance and participation are essential for satisfactory progress in this course.

2. **Completed Assignments**

   - Each student is responsible for completing all assignments on time.
   - All homework assignments, projects, questions, etc., are to be typed. Points will be taken off for grammar and/or spelling errors.

3. **Course Project**

   Each student is responsible for individually completing the course project during the entire length of the course. The project will be worked on each week in conjunction with the lab and homework assignments. The Instructor will present each student with a copy of the "Course Project" at the start of the course. Students will respond to the letter portion as outlined in the directions and guidelines portion and present their project paper to the Instructor for grading by Week or Unit 11, or according to the discretion of the Instructor. Instructors have the discretion of requiring an oral presentation with the documentation presentation.

Evaluation Criteria Table

The final grade will be based on the following weighted categories:

CATEGORY	WEIGHT
Labs	25%
Project	30%
Quizzes	15%
Final Exam	30%
Total	**100%**

Grade Conversion Table

Final grades will be calculated from the percentages earned in class as follows:

A	90 - 100%	4.0

B+	85 - 89%	3.5
B	80 - 84%	3.0
C+	75 - 79%	2.5
C	70 - 74%	2.0
D+	65 - 69%	1.5
D	60 - 64%	1.0
F	<60%	0.0

COURSE OUTLINE

Wk	Lesson Title	Content Covered
1	Introduction To Ethics and Cyber crime	**Part 1, Chapter 1** **Introduction to Cyber Crime and Security** • Define cyber crime • Identify various common types of cyber crime • Understand what makes something a cyber crime **Part 2, Chapter 9** **Introduction to Ethics** • Define ethics • Identify common ethical theories • Understand ethics as it relates to the Web
2	Ethics and Web Communications	**Part 2, Chapter 10 Networking** • Netiquette principles related to communication in cyberspace • Ethical issues related to free speech and dissemination of hate mail, chain letters, and pornographic literature in cyberspace • Code of ethics governing communication on the Web
3	Ethics and Cyber Content	**Part 2, Chapter 11 Intellectual Property** • Define intellectual property • Appropriate and inappropriate content available on the Web • Ethical issues related to intellectual property infringement in cyberspace • Code of ethics governing the publication and use of cyber content • Legal aspects of copyright and other intellectual property violations in cyberspace

4	Ethics and Privacy in Cyberspace and Encryption	**Part 2, Chapter 12** **Privacy** • Ethical aspects of the right to privacy in cyberspace • Privacy infringement in cyberspace • Code of ethics governing the conduct of Internet Service Providers and users • Legal aspects of privacy infringement in cyberspace **Part 1, Chapter 7 Encryption** • Define encryption • History of encryption • Modern methods of encryption • Using encryption to ensure privacy
5	E-Commerce Business Models and Concepts	**Part 3, Chapter 14: E-Commerce Business Models and Concepts** • Ethical issues involved in online commercial transactions • Should Web bugs be regulated?
6	Security and Encryption	**Part 3, Chapter 5** **Security and Encryption** • Secure online transactions • Using hackers to fight hackers • Case Study: VeriSign, “The Web’s security blanket” **Part 3, Chapter 15** **E-Commerce Payment Systems** • Paypal • Rocketcash • Payments over wireless systems • Case Study: CheckFree
7	Malicious Code	**Part 2 Chapter 13 Computer and Network Security** **Part 1, Chapter 8 Computer Security Hardware and Software** • Different types of malicious code • How malicious code evolves • Preventing virus attacks
8	Preventing Web Intrusions	**Part 1, Chapter 3 Assessing a Target System** **Part 1, Chapter 4** **Denial of Service Attacks** • Threat from intruders • Methods of intrusion • Causes of intruder attacks • Types of intrusion • Different mechanisms to control intrusion

9	Implementing Web Site Security	**Part 1, Chapter 6** **Basis of Assessing and Securing a System** **Part 1, Chapter 8 Computer Security Hardware and Software** • Need for Web site security • Role of Web servers in ensuring Web site security • Need for securing operating systems • Areas of security management • Functioning of IIS • Security loopholes in IIS and measures to counter them • Functioning of the Apache Web server • Security loopholes in the Apache Web server and measures to counter them
10	Future Trends in Web Security	**ITT Tech Virtual Library (student research from Unit 9)** • Need for security management • Role of QA in security management • Risks involved in outsourcing • Security risks to wireless technology **Students will use the ITT Tech Virtual Library to research the new security issue of their choice**. • They will then present their findings to the class for discussion.
11	**Review and Final Examination**	

INTENT/INTERFACE

This course enhances the students' learning process in the area of Web and network security; examining these issues from ethical, legal, and technological perspectives. The course uses the students' previously acquired knowledge in Web, network, and information technology security as a basis for examining the legal and ethical issues often overlooked in the educational process. Traditional ethical theories are introduced along with legal issues related to the intellectual property. The course project focuses on security issues at the server/operating system level.

