

SW 342 Internet Security at Home and at Work

Loop Campus, Wednesday, 6-9 pm

LeRoy Foster

Phone: (847) 723-2429

e-mail: lfoster@depaul.edu

Course Description

The main goal of the course is to provide students with a comprehensive overview of computer and network security issues including the numerous types of attacks computers are vulnerable to, the types of attacker profiles, and the hardware and software defense solutions available. The text begins with an overview of the subject including security goals, the importance of security, intruder profiles, and defense mechanisms. The topics subsequently covered include security and the individual personal computer in both the home and corporate environments. This includes protecting the single device from the threats of data theft, viruses and spyware, techniques of authentication and security patch management. Next, corporate security is presented including policy issues involving e-mail, Internet access, passwords, Incident Response and Disaster Recovery. Internet Security and Network Security are addressed focusing on the threats to WAN and LAN networks and methods of protecting each type of network. Finally, the last chapter pulls all of the concepts together, presenting a picture of "Total Security". While each chapter stands alone in terms of the specific topic it presents, the concepts in each chapter overlap into the other chapters. It is difficult to discuss protecting an organizational network or even an individual computer without addressing threats from the Internet. Students will learn to apply these concepts to each particular setting and know how and why they are adapted from one environment to another.

About the Instructor

Manager, Network Security and Regulatory Compliance, with an M.S. in computer science from the University of Chicago.

Course Prerequisites

Basic familiarity with the Windows 95/98 operating system. Note: You should have an Internet account prior to the beginning of class.

Competencies Offered

- H-2-C:** Can identify an organizational problem and design a plan for change based on an understanding of social science theories or models.
- S-3-A:** Can understand different perspectives on the relationship between technology and society, and describe the scientific principles underlying technological innovations.
- S-3-X:** Understands and can apply principles of internet security issues to the home computer environment.
- F-X:** Understands internet security issues and their relevance and application to the workplace environments

Learning Experience

Through lectures, discussions, lab work and written assignments, we will highlight the foundation for understanding the broader field of Information security. This accomplished by defining key terms, explaining essential concepts, and providing a review the origins of the field and its impact on the understanding of Information Security.

You will be asked to: 1) read the assigned readings for each class and locate additional material on your own; 2) participate in class discussions; 3) participate in computer lab assignments.

Textbooks and Other Required Reading Materials

- Mark Ciampa, *Security Awareness: Applying Practical Security in Your World, Second Edition* Course Technology , ISBN 1-4188-0969-1
- Various articles to be distributed in class

SW 342 Internet Security at Home and at Work

Assignments

- A final paper tailored to your interests and relating to the competencies you've selected. The paper will be primarily analytical. If you register for one competence, you should plan to write a paper or approximately 5-7 pages. If you register for two competencies, you may write separate papers for each, or a single paper of 10-12 pages relating to both competencies.
- Hands –On Learning at the end of each chapter, students find a chapter summary and review questions as well as exercises and case exercises, which give them the opportunity to examine the information security arena outside the classroom. Using the exercises, the student can research, analyze and write to reinforce learning objectives and deepen their understanding of the text. With the case labs/exercises, students use professional judgment, powers of observation and elementary research, to create solutions for simple information security scenarios.

Grading & Assessment	
10% of the grade is based on quizzes. Quizzes are announced one day in advance and may vary from 3 to 5 questions that may be in any format.	
10% of the grade is based on keeping a project notebook. Students are asked to obtain a small notebook or use a lab notebook and keep notes on the results of each of the assigned hands-on projects located at the end of each chapter. The notes should include comments that you can use once the class is over to help describe dialog box results, to keep copies of the network diagrams you make, to retain information on configuration parameters and their meanings, to describe alternative steps, and other information pertinent to the projects.	
40% of the grade is based on completing the end of chapter case project assignments. An electronic version of the case project assignments can be downloaded from the course's Web site.	
Final Paper	40%
TOTAL	100%

FINAL PAPERS will be evaluated on the basis of the following:

- Content: Detailed and insightful discussion of the chosen topic, using relevant example and support from course readings, class discussion, personal experience, and (where appropriate) outside research.
- Organization: Clear thesis statement, logical development of main points, and well structured paragraphs.
- Stylistics: Logical sentence structure, grammar, and punctuation; careful proofreading; appropriate documentation of outside sources.