

**SUNY INSTITUTE OF TECHNOLOGY
MARCY CAMPUS
P.O.BOX 3050
UTICA, NEW YORK 13504-3050
SCHOOL OF INFORMATION SYSTEMS & ENGINEERING TECHNOLOGY**

FALL 2012

NCS 181 – INTRODUCTION TO CYBER SECURITY

INSTRUCTOR: Dave Climek

OFFICE ROOM: Donovan 1215

OFFICE TELEPHONE NO: 315-792-7284

EMAIL: climekd@sunyit.edu

OFFICE HOURS: Monday and Tuesday 4:00PM - 6:00PM and appointments by request

REQUIRED TEXTS:

(S) Essential Computer Security by T. Bradley and H. Carvey, Syngress Publishing:
ISBN: 1597491144; (2006)

AND

(B) Complete Guide to Internet Privacy, Anonymity & Security, Matthew Bailey, Nerel
Online (July 30, 2011), ISBN-10: 3950309306, ISBN-13: 978-3950309300

RECOMMENDED READING: The student should have access to the Internet and World Wide Web. There are also several magazines and journals that may be used as sources of material for this course. You will be required to keep abreast of current events in this field. Reading and written assignments will be required utilizing the aforementioned reference sources.

COURSE OVERVIEW: Introduction to the field of cyber security. The kinds of information system security threats that might be faced by home and/or small business users and prudent security countermeasures used to counteract them are covered. Security issues faced by users of information systems will be explained as well as the potential damage they may cause. Provides the student with knowledge necessary to protect themselves against many of the information systems security threats faced in everyday life.

COURSE OBJECTIVES: Upon completion of the course, the student will have a basic understanding of the fundamentals of cyber security, including the issues associated with cyber security on home and/or small business systems. Furthermore, the student should be able to utilize a variety of resources and tools to advance their studies in cyber security, learning how professionals go about gaining new knowledge and keeping current with change.

SPECIFIC COURSE OBJECTIVES: At the end of this course, the successful student will:

- Understand the basic terminology associated with the cyber security field,
- Be able to describe the various cyber security issues facing Information System users,
- Be able to identify potential security practices to increase safe computing,
- Be familiar with the basic designs of computers and operating systems,
- Be aware of various careers choices and job opportunities in the cyber security field.

METHOD OF INSTRUCTION: This course will be conducted in a lecture/discussion format. Assigned reading, visual aids, supplementary reading (handouts) and independent research may also be used. If time and opportunity permits, guest lecturers and/or field trips may be included.

COURSE ETHICS: Student collaboration on reading assignments, studying for assessments and finding homework sources is acceptable and encouraged. Students are expected to hand in their own original work on Assessments, Homework Assignments, and Technology Papers. SUNYIT HAS, IN THE PAST, DISCIPLINED, EXPELLED, AND EVEN PROSECUTED STUDENTS WHO HAVE ATTEMPTED TO ILLEGALLY ACCESS, MODIFY AND/OR VANDALIZE COMPUTER AND NETWORK SYSTEMS. ILLEGAL ACTIVITIES BY STUDENTS IN THIS CLASS INVOLVING ANY COMPUTERS OR NETWORKS, ANYWHERE, WILL NOT BE TOLERATED.

COURSE GRADING COMPONENTS:

In-class Assessments (3)	= 60%
Attendance (14)	= 10%
Homework Assignments (10)	= 10%
Technology Paper (1)	= 20 %
Total	= 100 %

Homework assignments are due the day listed below. Ten points will be lost for every day late unless prior arrangement is made with instructor. **Assignments that are turned in 10 days or more past the assigned due date will not be accepted and will be awarded a zero (0) grade.**

COURSE OUTLINE

(Tentative - May be revised as school calendar and class meetings dictate. Students will be advised of changes)

Week 1 (8/27): INTRODUCTION: SECURITY SURVEYS, ETHICS
S (1), B (1)

(9/3): LABOR DAY – NO CLASS

Week 2 (9/10) PC, SOFTWARE, NETWORK, PROTOCOL BASICS
S (Appendix A)
HW 1 DUE

Week 3 (9/17): PROTOCOLS CONTINUED, APPLICATIONS

S (Appendix A)

HW 2 DUE

Week 4 (9/24): ASSESSMENT 1

Week 5 (10/1): ATTACKS 1: HACKING

B (2, 4)

HW 3 DUE

SUBMIT PAPER TOPIC

MID-SEMESTER BREAK (10/8-10/9)

Week 6 (10/15): ATTACKS 2: DOS, MALWARE

S (3), B (6)

HW 4 DUE

Week 7 (10/22): SPAM, PHISHING, SOCIAL NETWORKING

S (6, 7, 9), B (5, 10, 11)

HW 5 DUE

Week 8 (10/29): ASSESSMENT 2

Week 9 (11/5): BASIC SECURITY CONCEPTS 1: VULNERABILITY ASSESSMENT, SYSTEM HARDENING, DEFENSE IN DEPTH

S (4, 10) B (7)

HW 6 DUE

Week 10 (11/12): BASIC SECURITY CONCEPTS 2: PASSWORDS, ANTIVIRUS, ANTISPYWARE, FIREWALLS

S (2, 5, 9, Appendix B), B (3, 8)

HW 7 DUE

Week 11 (11/19): ENCRYPTION

S (7), B (13)

HW 8 DUE

Week 12 (11/26): INTRUSION DETECTION/PREVENTION SYSTEMS, SAFE COMPUTING, POLICY AND EDUCATION

S (5, 6, 11) B (15)

TECHNOLOGY PAPER DUE

Week 13 (12/3): STEGANOGRAPHY, LAWS, FORENSICS, INCIDENT INVESTIGATION, BIOMETRICS

HW 9 & 10 DUE

Week 14 (12/10): ASSESSMENT 3

HOMEWORK ASSIGNMENTS

1. Submit assignments to our class webpage electronically via Angel. They should be written in double-spaced, typewritten pages, of uniform margins, with correct grammar, spelling and syntax.

2. Use textbooks, professional journals, newspapers, magazines, WWW and Internet.

DOCUMENT YOUR SOURCES.

3. Each assignment will be done according to the format discussed in class.

4. Assignments should be submitted the day that they are due. Ten points will be lost for every day late unless prior arrangement is made with instructor. **Assignments that are turned in ten days or more past the assigned due date will not be accepted and will be awarded a zero (0) grade.**

5. Please use the following Format (separate page each)

Title Page (see below for format)

Item I What the assignment asked you to do or show --- What were you asked to do?

Item II What you (the student) did (the steps that were followed) --- What did you do?

Item III What you learned (This should be a summarization of what you found out --- What was the key cyber security principle that was demonstrated in this assignment? --- What did you learn?--- Why is this important?) This should be a summarization of what you found out; in your own words.

List of References

(PLAGIARISM WILL RESULT IN POINT LOSS AND THE POTENTIAL FOR A GRADE OF ZERO (0) FOR THE ASSIGNMENT). You must document the source(s) used for the assignment.

(Sample Title Page Format)

NCS 181

Introduction to Cyber Security

Homework Assignment #1

Date Due

Student Name

TECHNOLOGY PAPER

1. Get research topic approved no later than Week 5. Suggested areas of research will be listed on the class web site.

2. Research and describe your chosen area using a number of sources, including textbooks, magazine articles, the World Wide Web, Internet, etc.
 3. An approximately 10 - 15 page, double-spaced paper (exclusive of title, table of contents, list of references, etc. – i.e., 1500 to 2500 words) is due by Week 12. Submit via Angel. You may hand in a **draft paper copy** earlier (no later than Week 8) if you want commentary and suggestions. Ten points will be lost for every day late unless prior arrangement is made with instructor. **Assignments that are turned in ten days or more past the assigned due date will not be accepted and will be awarded a zero (0) grade.**
 4. You must use the following format for the paper:
 - Title Page (see below for format)
 - Table of Contents
 - Introduction
 - 1 to 5 Sections of Information
 - Summary
 - List of References (You must document the sources used for the paper).
 5. The paper will be evaluated for, among other things, plagiarism. **Papers with greater than 30% plagiarism will have their grade reduced by the determined amount.**
-

(Sample Title Page Format)

NCS 181

Introduction to Cyber Security

Date Due

Student Name

This course is also offered under the articulation agreement between Binghamton University and SUNYIT. It is available to qualified students at Binghamton University via the distance learning system Enginet.