



# From Hackers to CEOs: An Introduction to Information Security ITP 499 (2 Units)

---

<b>Objective</b>	Upon completing this course, students will: <ul style="list-style-type: none"> <li>- Understand the fundamentals of information security</li> <li>- Learn the basics of securing a workstation</li> <li>- Understand basic networking and security technologies</li> <li>- Understand the relationship between security and management</li> </ul>
<b>Concepts</b>	This course is designed to be an introductory course in information and computer security. This course starts with an analysis of threats to information integrity. Students will then get an introduction to security mechanisms and policies. Students will learn how security infrastructure will integrate with the rest of the business and IT infrastructure, through the use of hands-on projects.
<b>Prerequisites/ Recommended Preparation</b>	None
<b>Instructor</b>	Joseph Greenfield
<b>Contacting the Instructor</b>	joseph.greenfield@usc.edu   213-740-4604
<b>Office Hours</b>	2:00 – 5:00 Monday, OHE 530C or by appointment
<b>Lecture</b>	3:30 – 5:00 Tuesday, KAP 160
<b>Lab</b>	3:30 – 5:00 Thursday, KAP 160
<b>Required Textbooks</b>	<i>Principles of Computer Security</i> . Conklin, White, Cothren, Williams, and Davis. McGraw Hill, 2004. ISBN: 0-07-225643-5
<b>Web Site</b>	All course material will be on Blackboard at <a href="http://blackboard.usc.edu">blackboard.usc.edu</a>
<b>Grading</b>	Grading will be based on percentages earned in assignments. Students will have structured labs throughout the semester, to be conducted during the scheduled lab time. In addition, students will work in groups to prepare a 20-minute presentation on a topic of their choosing. The presentations will be conducted during the last few weeks of class.  <div style="display: flex; justify-content: space-between;"> <div style="width: 60%;">Labs</div> <div style="width: 30%;">40%</div> </div> <div style="display: flex; justify-content: space-between; margin-top: 5px;"> <div style="width: 60%;">Presentation</div> <div style="width: 30%;">20%</div> </div> <div style="display: flex; justify-content: space-between; margin-top: 5px;"> <div style="width: 60%;">Midterm</div> <div style="width: 30%;">15%</div> </div> <div style="display: flex; justify-content: space-between; margin-top: 5px;"> <div style="width: 60%;">Final</div> <div style="width: 30%;">25%</div> </div> <div style="display: flex; justify-content: space-between; margin-top: 5px;"> <div style="width: 60%;">Total</div> <div style="width: 30%;">100%</div> </div>
<b>Policies</b>	<ul style="list-style-type: none"> <li>- Projects turned in after the deadline will automatically have 5% deducted per day. Projects will not be accepted after 1 week beyond the project's deadline</li> <li>- No make-up exams (except for medical or family emergencies) will be offered nor will there be any changes made to the Final Exam</li> </ul>

	<p>schedule.</p> <ul style="list-style-type: none"> <li>- It is your responsibility to submit your project on or before the due date. <b>It is not the responsibility of the lab assistant.</b> Do <b>not</b> turn in anything to your lab assistant!</li> <li>- All projects will be digitally submitted through blackboard except where specifically specified. Always keep a backup copy of your labs</li> </ul>
<p><b>Academic Integrity</b></p>	<p>The use of unauthorized material, communication with fellow students during an examination, attempting to benefit from the work of another student, and similar behavior that defeats the intent of an examination or other class work is unacceptable to the University. It is often difficult to distinguish between a culpable act and inadvertent behaviour resulting from the nervous tension accompanying examinations. When the professor determines that a violation has occurred, appropriate action, as determined by the instructor, will be taken.</p> <p>Although working together is encouraged, all work claimed as yours must in fact be your own effort. Students who plagiarize the work of other students will receive zero points and possibly be referred to Student Judicial Affairs and Community Standards (SJACS).</p> <p>All students should read, understand, and abide by the University Student Conduct Code listed in SCampus, and available at:  <a href="http://www.usc.edu/student-affairs/SJACS/nonacademicreview.html">http://www.usc.edu/student-affairs/SJACS/nonacademicreview.html</a></p>
<p><b>Students with Disabilities</b></p>	<p>Any student requesting academic accommodations based on a disability is required to register with Disability Services and Programs (DSP) each semester. A letter of verification for approved accommodations can be obtained from DSP. Please be sure the letter is delivered to me (or to your TA) as early in the semester as possible. DSP is located in STU 301 and is open 8:30 a.m. - 5:00 p.m., Monday through Friday. The phone number for DSP is (213) 740-0776.</p>

# Introduction to Information Security

## ITP 499 (2 Units)

---

### Course Outline

#### **Week 1** – Introduction to Computer Security & Hackers

- Course overview
- What is a hacker?
- I'm being hacked!?!
- Hacker methodology

**Reading:** Chapter 1

#### **Week 2** – Security Concepts

- Confidentiality, Integrity, and Authority
- Least Privilege
- Security Vocabulary
- Basics of Defense

**Reading:** Chapter 2

#### **Week 3** – Windows vs. Linux vs. Mac

- Benefits & trade-offs
- Histories of each
- How to get them all working together ☺

**Reading:** Instructor Notes

**Lab 1:** Installing an OS from Scratch

#### **Week 4** – Network Technology

- OSI 7-layer model
- TCP model
- Overview of networked systems

**Reading:** Chapter 9

**Lab 2:** Port Scanning

#### **Week 5** – Network design and topology

- Overview of physical & logical topologies
- "Secure" topologies
- DMZ layer
- Security devices

**Reading:** Chapter 10

**Lab 3:** Vulnerability Assessment

## **Week 6** – Legal Issues

- Overview of legal issues with information security
- Sarbanes-Oxley
- HIPAA
- CA disclosure law
- What do I need to do vs. what should I do?

**Reading:** Chapter 24

**Lab 4:** Your First Hack!!!

## **Week 7** – Policy

- Security Policies
- How to write a policy?
- How to implement a policy?
- Why do we have or need policies?

**Reading:** Chapter 19

## **Week 8** – Risk Analysis

- How to determine what is at risk?
- Who to tell & how to tell them
- Risk mitigation and prevention

**Reading:** Chapter 20

## **Week 9** – MIDTERM

### **Week 10** – Access Control, Permissions & Passwords

- How do we limit access?
- How do we enforce our policies?
- Passwords: Good, bad, and ugly

**Reading:** Chapter 14

**Lab 5:** Breaking Passwords

### **Week 11** – E-mail & Phishing

- “We need to verify your account...”
- E-mail threats
- Detecting phishing scams
- What to do when you’ve been scammed?

**Reading:** Chapter 16

**Lab 6:** Spoofing e-mail

### **Week 12** – Viruses, Spyware, and Malware

- History of Viruses
- What’s dangerous out there
- How do we get rid of the nasty things on our computer?

**Reading:** Chapter 15 & Instructor Notes

**Lab 7:** Basic Windows Workstation Security

**Week 13** – Incident Response

- “I’ve been hacked!!! What do I do?”
- Introduction to Computer Forensics
- Response policies and practices

**Reading:** Chapter 23

**Lab 8:** Basic Computer Forensics Lab

**Week 14** – The Human Element

- Social Engineering 101
- Training personnel about security
- Interviewing and Interrogating

**Reading:** Chapter 4

**Week 15** – Conclusion

- Review for the final exam
- Conclusion to the course