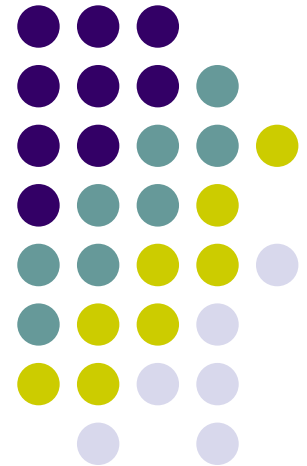


# Computer Security

UC Santa Cruz's Basic Overview  
Introduction

2009



# Navigating This Tutorial



This Computer Security Overview Training consists of 10 different self-paced modules that you can view in your web browser or download to your computer.

Each module is designed to take approximately 5-15 minutes to complete and includes a certificate at the end that you can print out and have signed.

Once you complete each module, you can go back to the ITS Security Awareness Training site ([http://its.ucsc.edu/security\\_awareness/training.php](http://its.ucsc.edu/security_awareness/training.php)) to view or download the next one. You can also visit this website at any time to review the information in these training modules or to take additional tutorials as they become available.

# Training Modules



## **1. Introduction to Computer Security**

**2. Social Engineering**

**3. Internet Privacy and Security**

**4. Practice “Safe Emailing”**

**5. Password Strength and Security**

**6. Ten Other Essential Security Measures**

**7. Protecting PII and Other Restricted Data**

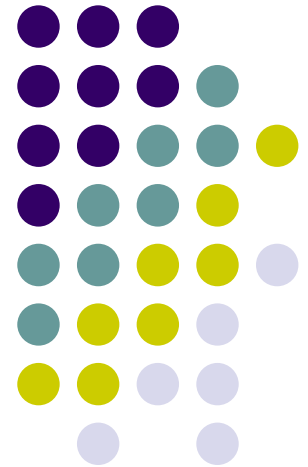
**8. Reporting IT Security Incidents**

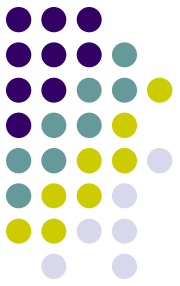
**9. Additional Information & Resources**

**10. Security Self-Test: Questions & Scenarios**

You are  
Here

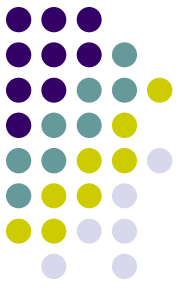
# 1. Introduction to Computer Security





# *What is Computer Security?*





# Computer Security is the protection of computing systems and the data that they store or access

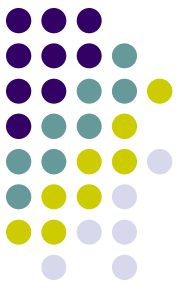


# Why is Computer Security Important?



## Computer Security allows the University to carry out its mission by:

- Enabling people to carry out their jobs, education, and research.
- Supporting critical business processes
- Protecting personal and sensitive information



## **Quiz: What could happen if my computer gets hacked?** *(select all that apply)*

- a) It could be used to hide programs that launch attacks on other computers.
- b) It could be generating large volumes of unwanted traffic, slowing down the entire system.
- c) Someone could be distributing illegal software from my computer, without my realizing it.
- d) Someone could access restricted or personal information on my computer (e.g. identity theft).
- e) Someone could record all of my keystrokes and get my passwords.

*See next page for answer*



**Of course, the answer is  
“All of the above.”**

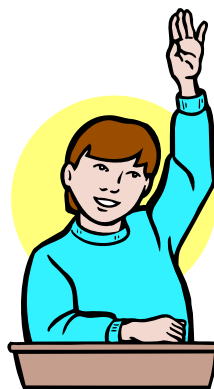
**A compromised computer can be used  
for all kinds of surprising things.**



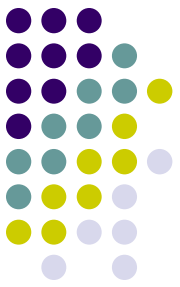


# Why do *I* need to learn about Computer Security?

## Isn't this just an IT Problem?



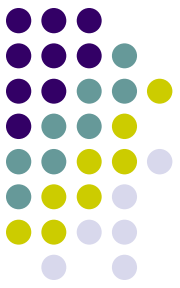
# Good Security Standards follow the “90 / 10” Rule:



- *10% of security safeguards are technical*
- *90% of security safeguards rely on the computer user (“YOU”) to adhere to good computing practices*

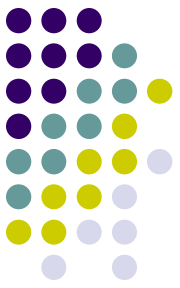
*Example: The lock on the door is the 10%. You remembering to lock the lock, checking to see if the door is closed, ensuring others do not prop the door open, keeping control of the keys, etc. is the 90%. You need both parts for effective security.*

# What Does This Mean for Me?



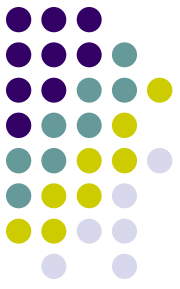
- *This means that everyone who uses a computer needs to understand how to keep their computer and data secure.*
  - *Information Technology Security is everyone's responsibility*
- *Members of the UCSC community are also responsible for familiarizing themselves and complying with all University policies, procedures and standards relating to information security.*
  - <http://its.ucsc.edu/security/policies/>

# Many cyber security threats are largely avoidable. Some key steps that everyone can take include:



- *Use good, cryptic passwords that can't be easily guessed - and keep your passwords secret*
- *Make sure your computers operating system are protected with all necessary security "patches" and updates*
- *Make sure your computer is protected with up-to-date anti-virus and anti-spyware software*
- *Don't click on unknown or unsolicited links or attachments, and don't download unknown files or programs onto your computer*
- *Remember that information and passwords sent via standard, unencrypted wireless are especially easy for hackers to intercept*
  - *To help reduce the risk, make sure web pages have https, (not http,) in the web address (URL) before you enter any sensitive information or a password.*
  - *Also avoid standard, unencrypted e-mail and unencrypted Instant Messaging (IM) if you're concerned about privacy*

# SEC-**U**-**R**-**IT**-Y Objectives



- *Learn “good computing security practices.”*
- *Incorporate these practices into your everyday routine. Encourage others to do so as well.*
- *Report anything unusual – Notify the appropriate contacts if you become aware of a suspected security incident.*

# What are the consequences for security violations?

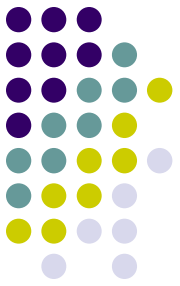


- *Risk to security and integrity of personal or confidential information*
  - *e.g. identity theft, data corruption or destruction, unavailability of critical information in an emergency, etc.*
- *Loss of valuable business information*
- *Loss of employee and public trust, embarrassment, bad publicity, media coverage, news reports*
- *Costly reporting requirements in the case of a compromise of certain types of personal, financial and health information*
- *Internal disciplinary action(s) up to and including termination of employment, as well as possible penalties, prosecution and the potential for sanctions / lawsuits*



# The different modules of this tutorial will:

- *Discuss the risks to your computer and the data it contains*
- *Provide additional guidelines for avoiding risks*
- *Suggest some practical and easy solutions*



# Would you like to:

(please click on an option)

Start again

Finish & go to the certificate

Select another lesson