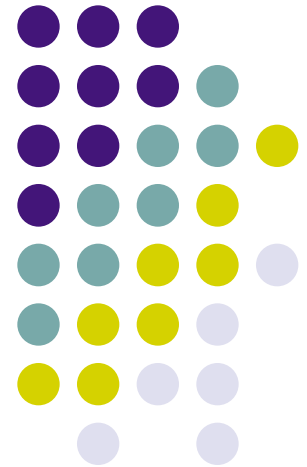


Introduction to Computer Security





What is Computer Security?

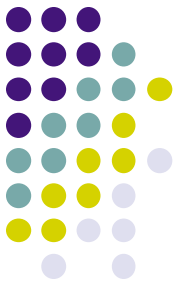




Computer Security is the protection of computing systems and the data that they store or access



Why is Computer Security Important?



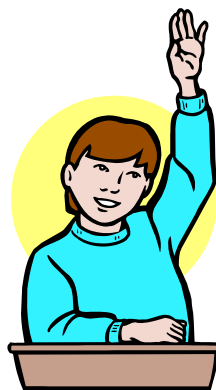
Computer Security allows the University to carry out its mission by:

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

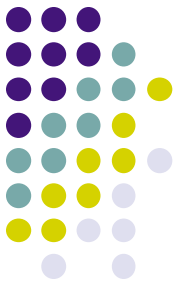


Why do *I* need to learn about Computer Security?

Isn't this just an IT Problem?



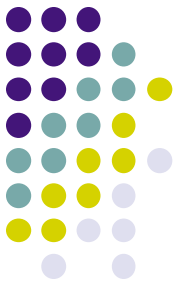
Good Security Standards follow the “90 / 10” Rule:



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

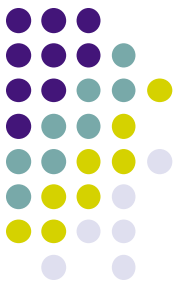
Example: *The lock on the door is the 10%. You remembering to lock the lock, checking to see if the door is closed, ensuring others do not prop the door open, keeping control of the keys, etc. is the 90%. You need both parts for effective security.*

What Does This Mean for Me?

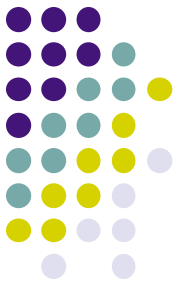


- This means that everyone who uses a computer or mobile device needs to understand how to keep their computer, devices and data secure.
 - *Information Security is everyone's responsibility*
- Members of the UCSC community are also responsible for familiarizing themselves and complying with all University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

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 your supervisor and the ITS Support Center if you become aware of a suspected security incident.



The Internet can be a hazardous place:



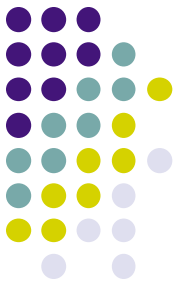
How many attacks to computers on campus do you think take place everyday?



- Thousands of attacks **per minute** bombard our campus network.
- An unprotected computer can become infected or compromised **within a few seconds** after it is connected to the network.



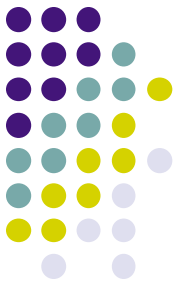
“I just keep finding new ways to break in!”



A compromised computer is a hazard to everyone else, too – not just to you.



Quiz: A hacked computer can be used to... *(select all that apply)*



- a) Record keystrokes and steal passwords.
- b) Send spam and phishing emails.
- c) Harvest and sell email addresses and passwords.
- d) Access restricted or personal information on your computer or other systems that you have access to.
- e) Infect other systems.
- f) Hide programs that launch attacks on other computers.
- g) Illegally distribute music, movies and software.
- h) Distribute child pornography.
- i) Generate large volumes of traffic, slowing down the entire system.

See next page for answer

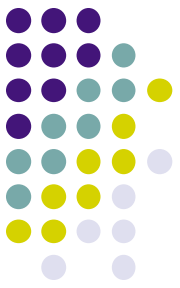
**Of course, the answer is
“All of the above.”**



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

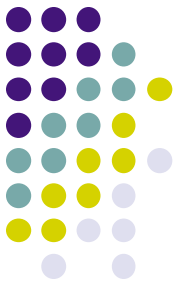


Many cyber security threats are largely avoidable. Some key steps that everyone can take include (1 of 2):



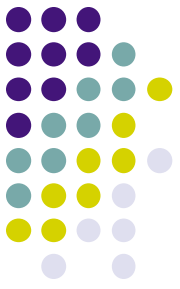
- Use good, cryptic passwords that can't be easily guessed - and keep your passwords secret
- Make sure your computer, devices and applications (apps) are current and up to date
- Make sure your computer is protected with up-to-date anti-virus and anti-spyware software
- Don't click on unknown or unsolicited links or attachments, and don't download unknown files or programs onto your computer or other devices

Key steps, continued (2 of 2):



- Remember that information and passwords sent via standard, unencrypted wireless are especially easy for hackers to intercept
 - *To help reduce the risk, look for “https” in the URL before you enter any sensitive information or a password (the “s” stands for “secure”)*
 - *Also avoid standard, unencrypted email and unencrypted Instant Messaging (IM) if you’re concerned about privacy*
- See ITS' Top 10 List and the other links on the training page for more.
 - *Top 10 List: <http://its.ucsc.edu/security/top10.html>*
 - *Training page: <http://its.ucsc.edu/security/training/index.html#cs>*

Protecting UCSC's Networks

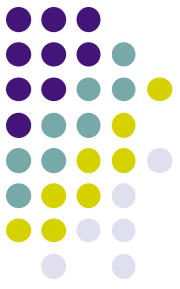


Computers posing a serious threat will be blocked or disconnected from the campus network. Passwords known to be compromised will be scrambled.

From UCSC's "Procedures for Blocking Network Access" (<http://its.ucsc.edu/policies/blockingproc.html>):

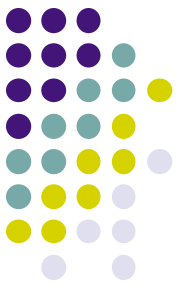
"Campus network and security personnel must take immediate action to address any threats that may pose a serious risk to campus information system resources.... If the threat is deemed serious enough, the account(s) or device(s) presenting the threat will be blocked or disconnected from network access."

What are the consequences for security violations?

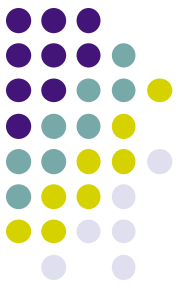


- Risk to security and integrity of personal or confidential information
 - e.g. identity theft, data corruption or destruction; lack of availability of critical information in an emergency, etc.
- Loss of valuable business information
- Loss of employee and public trust, embarrassment, bad publicity, 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 links on ITS' Security Training page will:



- Discuss the risks to your computer and portable devices and the data they contain
 - Provide guidelines and tips for avoiding common computer security risks
 - Suggest some practical and easy steps for keeping your information and devices safe
- <http://its.ucsc.edu/security/training/index.html#cs>



GETTING HELP:

If you have questions, please contact the ITS Support Center:

- Online: <http://itrequest.ucsc.edu>
- Email: help@ucsc.edu
- Phone: 831- 459-HELP (4357)
- In Person: 54 Kerr Hall, M-F, 8AM to 5PM
- Web Page:
<http://its.ucsc.edu/get-help/index.html>