

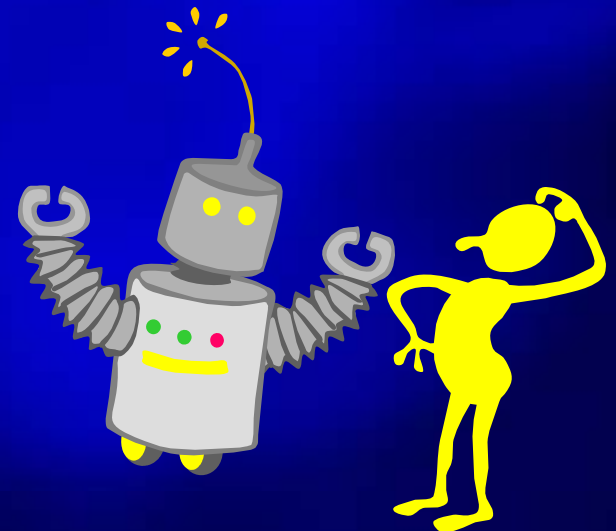
# All aboard the Cool Security Express



# Cool Careers

➤ **What are some Cool Careers and Why?**

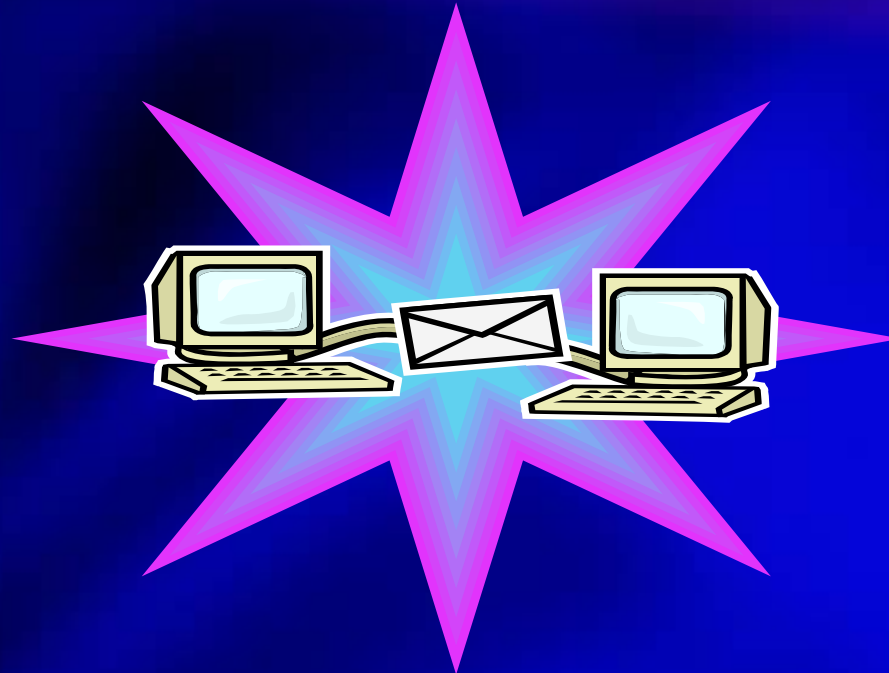
- ▣ **Lawyers, Doctors**
- ▣ **Astronaut**
- ▣ **Video Game Designer/Animator**
- ▣ **Athlete**



# What is Information Assurance

- ❑ Protects and Defends information & Information Systems
- ❑ How? Ensuring proper measures are in place
- ❑ Security = Pro-Active

# Lesson 1:



## The Internet





# What is the Internet?

**What is the Internet?**

**What is an Internet Service Provider (ISP)?**

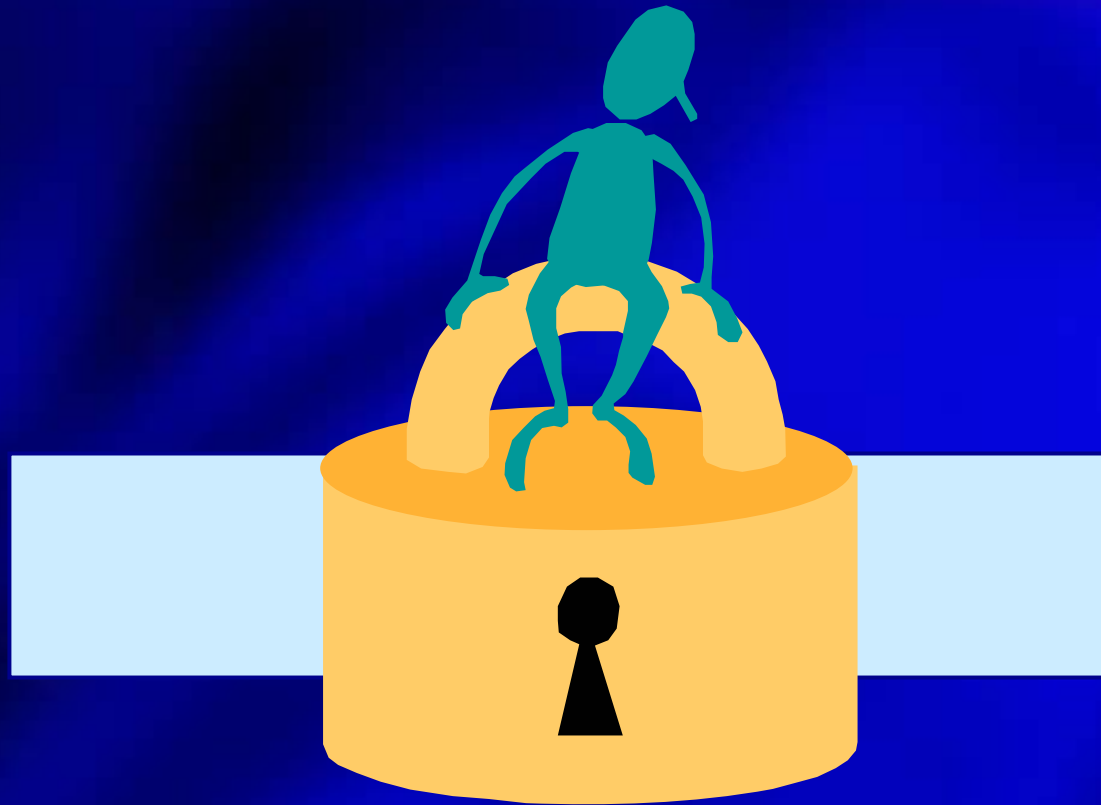
# The World Wide Web

WWW opens the World  
to you - and you to the  
World!



The WWW is a universal  
database of common  
information available to the  
entire Internet community

# Consider Security



Security should be considered in the early stages!



**DISCOVER  
SECURITY  
NEEDS**

# Lesson 2:

## Understanding the Hacker



# The Hacker: Who is He?

- **Characteristics of a Hacker:**
  - ▣ Usually male; age = 12-28 yrs.
  - ▣ Highly intelligent, but not a good student
  - ▣ Misunderstood by many
  - ▣ History of dysfunctional family
  - ▣ Have trouble getting dates
  - ▣ Very pleasant
  - ▣ Work in the computer field

# What Hackers Do:

## ➤ System Hacking

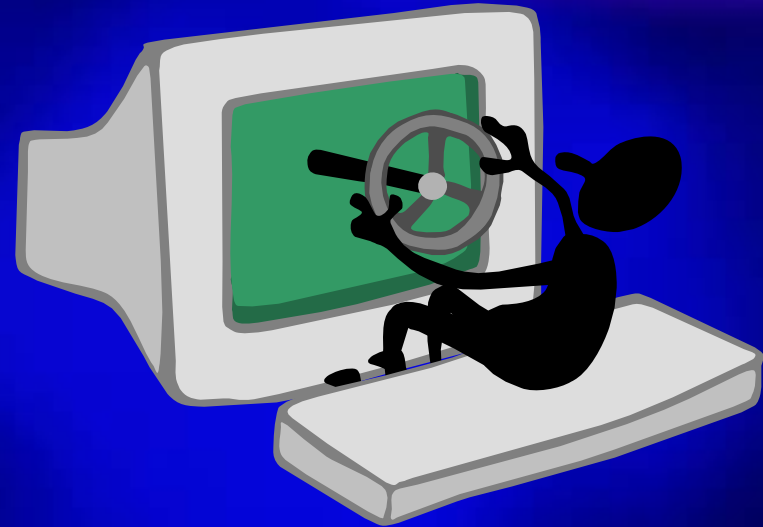
- ▣ Packet Sniffing
- ▣ Password Guessing

## ➤ Phreaking

- ▣ The Blue Box
- ▣ The Red Box

## ➤ Hacking with No machines

- ▣ Social Engineering
- ▣ Trashing



# Lesson 3:

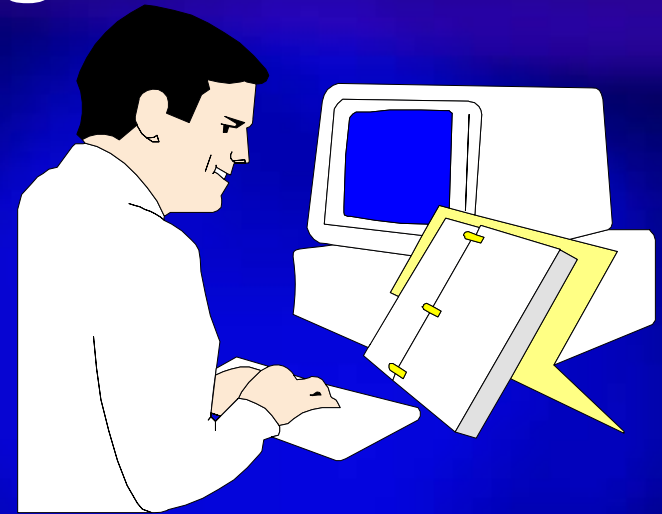


## The Hacker's Move



# How the Hacker gets In

## ➤ The Attacker

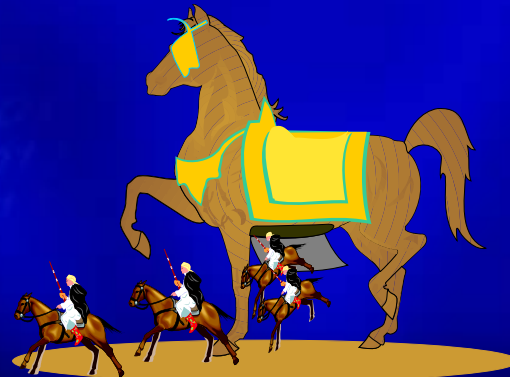
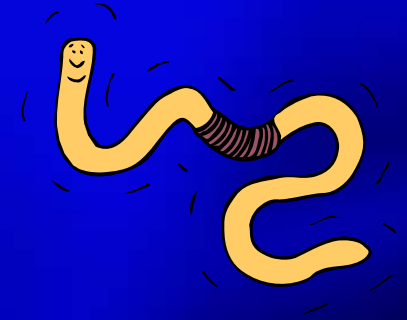


- ❑ **Denial of Service (DoS) attack**  
Makes a connection to the server and then floods your server with more request than it can handle
- ❑ **IP attacks (Spoofing)** where a user is induced into taking an incorrect action by giving it incorrect information
- ❑ **Piggy-backing** where a user leaves a session open or incorrectly logs off, enabling an attacker to resume the session
- ❑ **Malicious code (Viruses, Trojan Horses and Worms)** that causes destruction of information on computers

# Malicious Code

➤ malicious codes include:

- ▣ Virus
- ▣ Trojan Horses
- ▣ Worms



# Most Common Attacks

## ➤ Malicious Code:

- Virus - a computer program that “infect” other program in order to perform malicious action
- Trojan Horse - a program that pretends to be something else (I.e., you might download what you think is a new game, but when you run it, it deletes files from your hard drive)



# Most Common Attacks (con't)

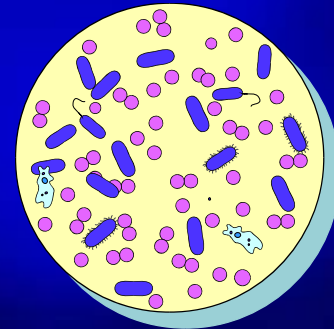
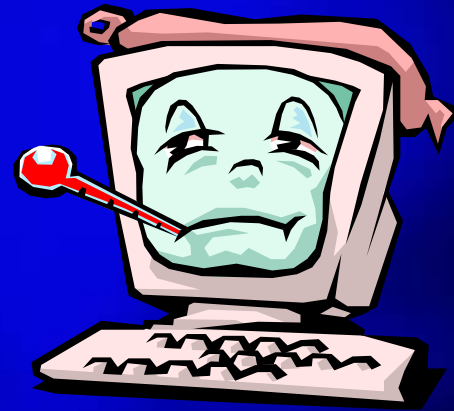
## ➤ Malicious Code :

- ❑ Worm a program that spread copies of themselves to computers throughout a network
- ❑ Can hide programs in email attachments
- ❑ Can spread unwanted files that cause damage to the user's computer and others
- ❑ Usually have friendly names, such as "I Love You"



# Virus Indicators

- Note Abnormal or Unexpected Activity
  - ▣ Displays, Music or Other Sounds
  - ▣ Slowdown in Processing Speed
  - ▣ Error Messages
  - ▣ Changes in File Sizes
  - ▣ Loss of Programs or Data
  - ▣ New File Names or dates Appear
  - ▣ Unexpected Messages





# Why Viruses are Successful?

- Lack of Awareness
- No Security Controls or Ineffective ones
- Bugs in Software
- Unauthorized Use
- Network Misuse
- Failure to get HELP when you suspect a virus attack
- No Norton or McAfee Live Updates



# Lesson 4:



## Securing Your Computer



# Password Management

- **Strong Password (combination of letters and characters, #\$\$%^&\*())**
- **Do not write it down**
- **Don't make it too hard to remember**
- **Don't use your internal password on external websites**
- **Never share a password**

Please Enter Your Password:

\*\*\*\*\*

# Anti-Virus Software

- **Recommended: Norton or McAfee**
- **Protects computers from viruses and other malicious code**
- **Configured to run automatically**
- **Software must be updated constantly to keep up with new viruses**



# Firewalls

Characterize  
System

- A Personal Firewall places a barrier between the Internet and your computer, helping to block hackers from accessing your computer.
- Every time your computer is probed or attacked, you get detailed reports and clear follow-up options.

Reports used to report hacker activity to assist law enforcement

# Intrusion Detection

- Intrusion refers to an actual illegal or undesired entry into an computer
- A system used to monitor network traffic to detect intrusions that have passed through a firewall
- It compares known attack signatures via databases or normal usage profiles



# Cool Careers in Information Assurance

- Physical Security** – access control, close circuit TV, state-of-art technology; salary range: \$35,000 - \$65,000
- Information Security** – securing data (collection, marking, disseminating, disposal); salary range: \$30,000 - \$140,000
- Personnel Security** – background investigations, drug testing, security clearance, and adjudicating results; salary range: \$35,000 - \$85,000

# Cool Careers in Information Assurance

(cont')

- Information System Security** – protect confidentiality and reliability of data (against hackers, virus, other threats); salary range: \$40,000 - \$140,000
- Homeland Security** – protection of U.S. borders (airspace, bio and chemical attack, cyber attacks); salary range: \$30,000 - \$120,000
- Critical Infrastructure Protection** – protecting telecommunication systems, nuclear plants, bridges (transportation system), food plants; salary range: \$30,000 - \$95,000



# List of Security Alerts: Seclists.org

- **Nmap Hackers** – list for security announcements, update patches, etc..
- **Carnegie Mellon (SEI) – CERT Coordination Center** – post all vulnerability reports, security alerts, incidents reported, hotline calls at:  
[www.cert.org/stats/cert\\_stats.html](http://www.cert.org/stats/cert_stats.html)
- **Bugtraq** - Premier security mailing list – announcement of vulnerabilities
- **Security Basics** – list of questions and allows one to ask basic security questions
- **Firewall Wizards** – Tips and tricks for how to install and monitor a firewall
- **Incidents** – list of actual security incidents (topics: trojans, worms, virus; what are they?)
- **Security Jobs** – popular list for advertising or finding jobs in the security field

# Free Software to help:

- Prevent Spam – Spam Nullifier – download at [www.spamnullifier.com](http://www.spamnullifier.com)
- Spyware – Spyware Doctor 3.5 –  
[www.pctools.com/offers/avsd/?ref=google\\_combo](http://www.pctools.com/offers/avsd/?ref=google_combo)
- Virus Provention – Dr. Web for Windows -  
[old.antivir.ru/english/dsav\\_toolkit/drweb32.htm](http://old.antivir.ru/english/dsav_toolkit/drweb32.htm)
- Firewall – F-prot used only for personal computers - [www.f-prot.com/download/home\\_user/](http://www.f-prot.com/download/home_user/)