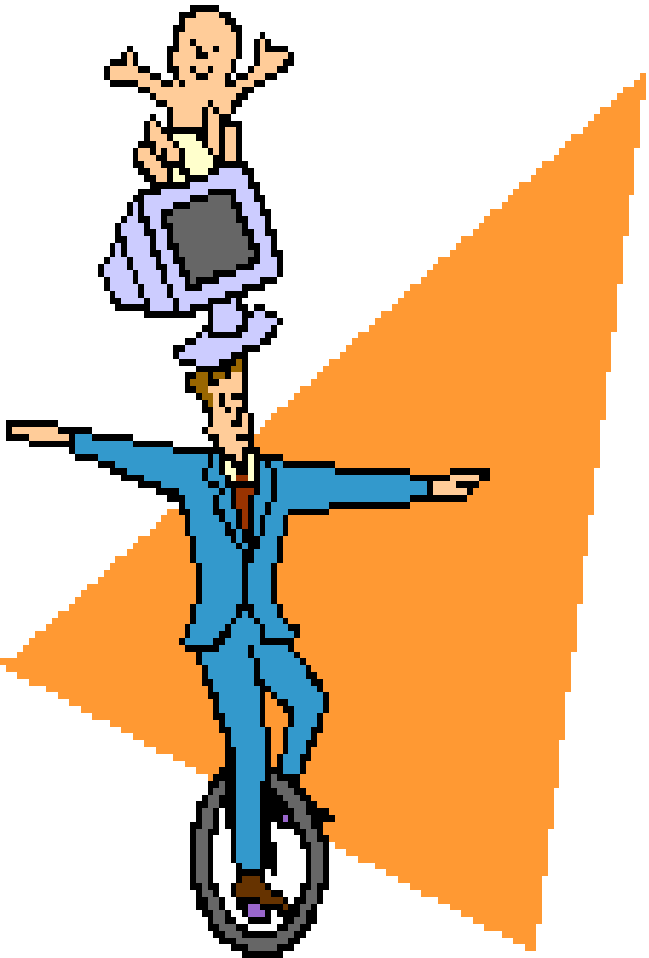


# Information Security Training for LSU Employees and Students



**Be good to your computer!**

# What is an END USER?

- An End User is any Employee or Student who uses the LSU Computer infrastructure in the course of their work

# You are responsible for:

- LSU Security Policies
- Using computer resources responsibly
- Using the computer for authorized purposes only
- Participating in the protection of electronic resources and data

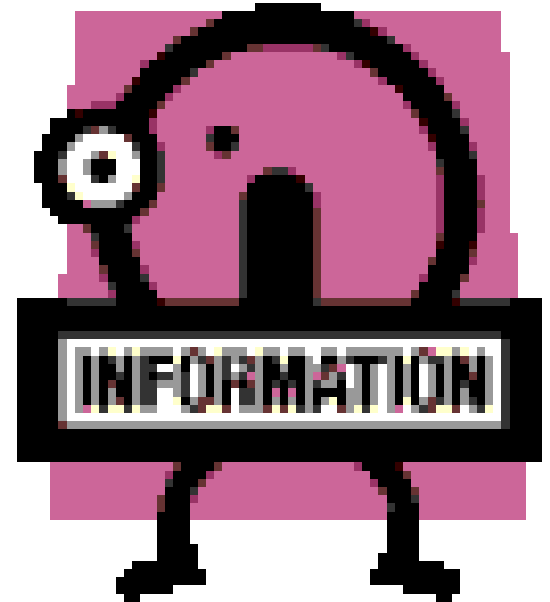
# I.T.'s Goal for Training

- Teach about information security
- Teach the role you play in protecting our network



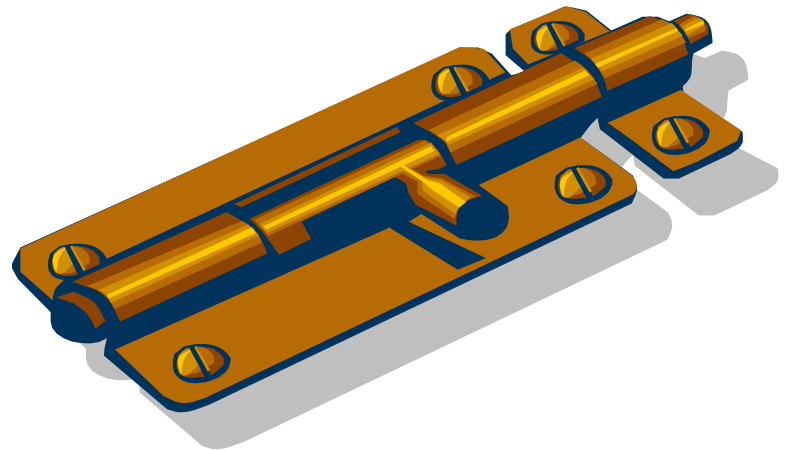
# What you need to know

- Passwords
- Malware
- Acceptable Use
- Social Engineering
- Confidentiality/Safeguards



# Passwords

- The use of a strong password is critical to secure protected information
- Your password is like the lock on your house (you want it to be as strong as possible)

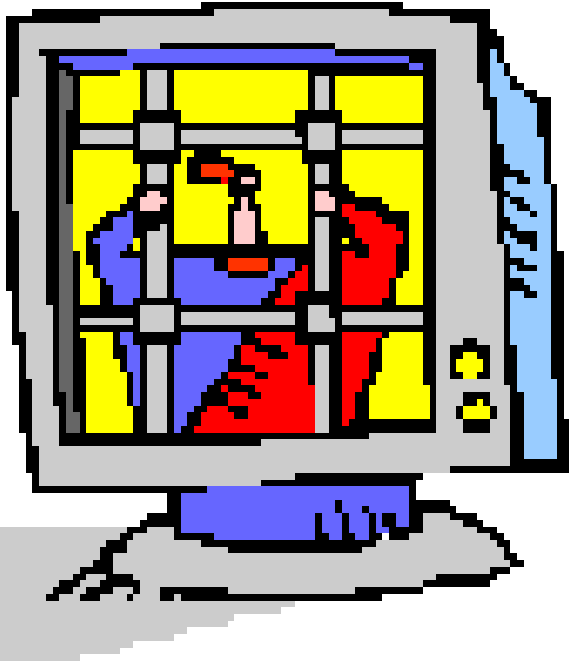


# **If Someone Knows Your Password They Can:**

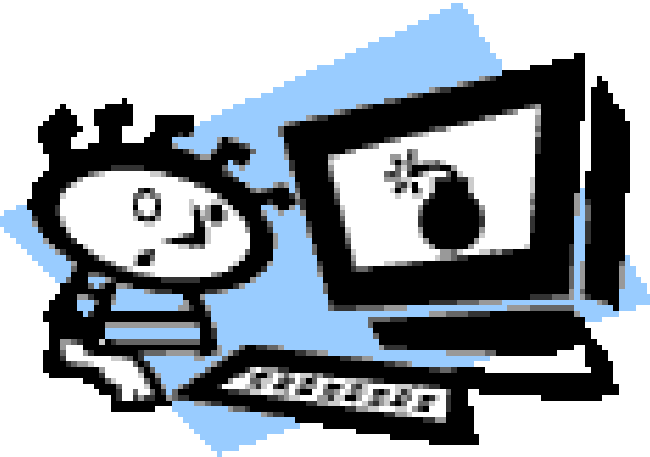
- Read your emails
- Respond to your emails as if they were you
- Inspect your files
- Have same access to all the information you have
- Have you blamed for offenses they commit

# If Someone Knows Your Password.....

They have  
stolen  
your  
identity!!!!



# Strong Passwords



- No password is unbreakable
- Given enough time and computing power a hacker can crack any password

# The Best Defense

- Choose passwords that take considerable time to break (given commonly available computing power)
- Change your password frequently (do not give a would-be hacker enough time to complete the cracking of your password)
- Never write down your password
- Never share your password



# The Characteristics of a Strong Password

- difficult to guess
- not found in the dictionary
- not based on some personal information
- contain characteristics from four different categories



# How Do I Create a Strong Password?

- The “**strength**” of a password is based upon the number of combinations possible:
  - 4 digit number –  $10^4$  or 10,000 possible combinations
  - 4 LC Alpha Char -  $26^4$  or 456,976 possible combinations
  - 8 LC Alpha Char –  $26^8$  or 208,827,064,576 possible combinations



# Time Needed To Crack Popular Passwords

- “LOVE” Dictionary 3 secs
- “43584927” Numbers <1 min
- “D0uBLeaGLe” 10 Alphanum 40 days
- “gAz1ll10n\$” 10 Alphanum 1.1 yrs  
U/L cases w/Spec.  
Char.

# Four categories to be included in passwords

Character Set Groups	Possible Characters	Possible Passwords (Min. of 8 characters)	Time Required to Try all Possible passwords (at 150 million attempts per second)
Lower case letters	26	$2.09 * 10^{11}$	20 min.
Mixed case letters	52	$5.34 * 10^{13}$	41 days
Mixed case letters, digits, and special characters	95	$6.63 * 10^{15}$	1.1 years
All above plus extended codes	222	$5.90 * 10^{18}$	1130 years

# How to make a Strong Password to Remember?

1. Take a popular saying like “A Fool And His Money Are Soon Parted.”
2. Take the first letter of each word “AFAHMASP”.
3. Capitalize consonants only “aFaHMaSP”.
4. Replace the “S” with “\$” “aFaHMa\$P”
5. Replace the “P” with “9” “aFaHMa\$9”

**Note: Do not use this example as your password**

# What do I do if I think my password has been compromised?

- Notify the help desk or your computer support personnel
- Change your password immediately (If you need assistance changing your password, ask your computer supporter)

## **Remember:**

you are responsible for all activities occurring under your LSU login ID



# Malware

- Malware is any software that causes unintended results
  - Examples of malware are:
    - viruses
    - worms
    - spyware
    - keystroke loggers
    - remote access Trojans



# Viruses



- Viruses are programs that attempt to spread throughout your system and the entire network
- **Prevention:**
  - antivirus software should be installed and updated on your computer

# Worms



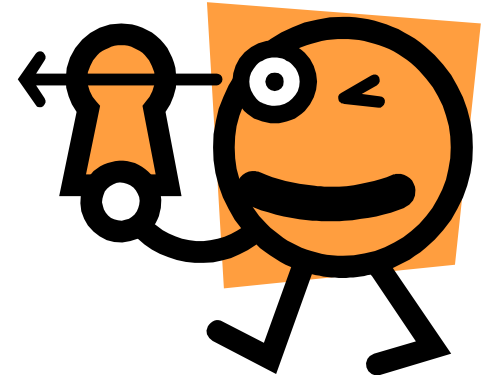
Worms spread without any user action. They usually take advantage of security holes in the operating system or software package

## Prevention:

- ensure that your system has all security updates installed



# Spyware

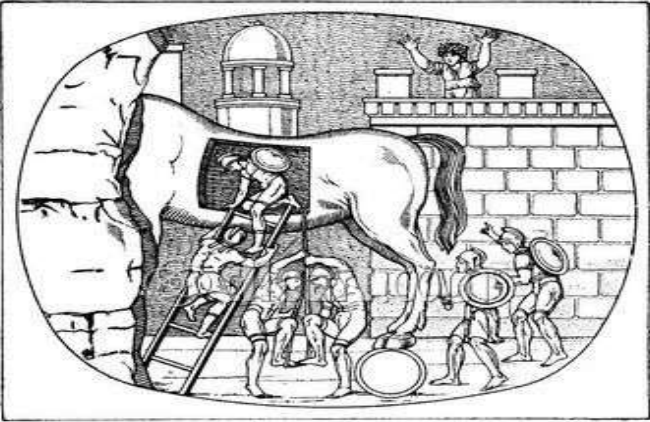


- Spyware is the class of programs that:
  - Monitor your computer usage habits and report them back to a company that stores this information in a database for marketing purposes
  - They are installed with little or no notification during the installation of another program or while browsing the Internet
  - Can also open advertising windows when browsing the Internet
- **To prevent spyware install and run an updated spyware scanner**



# Keystroke Loggers

- Keystroke loggers come in two varieties:
  - software programs that log every keystroke typed
  - hardware devices installed between your keyboard and computer
- Most antivirus programs and spyware scanners will detect software keystroke loggers
- Always check your hardware for anything unfamiliar



# Remote Access Trojans

Programs that allow remote users to connect to your computer without your permission who can then :

take screenshots of your desktop

take control of your mouse and keyboard

access your run programs at will

**Most antivirus programs will detect remote Access Trojans**

# Recognizing Malware

- Signs of Malware are:
  - reduced performance (your computer seems slow or “freezes”)
  - windows opening by themselves
  - missing data
  - slow network performance
  - unusual toolbars added to your web browser
- **Contact your computer supporter or the helpdesk if you suspect that your computer has malware installed**

# TAMPERED ACCOUNTS

- Indications that your account has been tampered with include:
  - a locked account
  - a password that is no longer accepted
  - missing data
  - computer settings that have unexpectedly changed
- Contact your computer supporter or helpdesk if you suspect that someone has tampered with your account



# Suspicious Email

- Suspicious email includes:
  - Any email you receive with an attachment
  - Any email you receive from someone you don't recognize
- Steps to combat malware from infecting your computer by email include:
  - disabling auto-preview and the preview panel in your email client
  - setting your email client to read all mail in plain text
  - saving all attachments to your computer and scanning them with your antivirus product before opening them

**If you suspect malware, contact your computer supporter or the helpdesk as soon as possible**

# Hoaxes

One type of suspicious email is the hoax. It warns of a virus or other type of malware that will cause serious harm to your computer such as erase the hard drive. It is especially perfidious because it usually comes from a well-meaning friend or relative who has been duped by the hoax.

# Hoax Characteristics

Hoax emails generally have the following characteristics:

- They are sent by a friend or colleague.
- They warn of a “new” virus or other malware.
- They claim new virus damages your computer in some catastrophic way, usually erasing the hard drive.
- The email claims that anti-virus programs are unable to detect it or have been caught off guard by its appearance.
- It urges your to send this “warning” to everyone in your address list.

# Problems Caused by Hoaxes

The main problem caused by hoaxes is that they overload email systems with unnecessary traffic. If the average internet user has 100 people in their address list and 1 million people are duped into sending the “warning”, that is 100 million unnecessary emails. Then another 100 million emails must be sent to notify everyone that the “warning’ was a hoax.

# Variations on Hoaxes

As with other threats hoaxes have developed variations. Some to watch out for are:

- The virus named in the hoax is the name of an actual virus. However, the real virus acts differently than what the hoax describes.
- The hoax will instruct you to delete an obscure system file causing your computer to malfunction on the next boot-up.

# How can you tell if it is a hoax?

It is a violation of CM-42 to re-transmit virus hoaxes. How do you determine whether a message is genuine or a hoax?

- Does the message have three or more of the characteristics of a hoax?
- Remember that any links in the message are there to convince you of its authenticity so don't rely on them.
- Enter specific or unique terms from the message into an internet search engine and see if any references to hoaxes come up.
- Call the help desk.

# How can you tell (cont.)

- Check the following websites:
  - <http://vil.mcafee.com/hoax.asp>
  - <http://www.snopes.com/computer/virus/virus.asp>
  - <http://antivirus.about.com/od/emailhoaxes//blenhoax.htm>

# Hoax Example

Here is an example of a virus hoax email:

Hi Everyone!

I checked this out and it is true!!!! Be careful what you open out there

I checked with Norton Anti-Virus, and they are gearing up for this virus! I checked snopes.com<<http://snopes.com/>>, and it is for real!! Get this E-mail message sent around to your contacts ASAP. PLEASE FORWARD THIS WARNING AMONG FRIENDS, FAMILY AND CONTACTS!

You should be alert during the next few days. Do not open any message with an attachment entitled "POSTCARD," regardless of who sent it to you. It is a virus which opens A POSTCARD IMAGE, which 'burns' the whole hard disc C of your computer. This virus will be received from someone who has your e-mail address in his/her contact list. This is the reason why you need to send this e-mail to all your contacts. It is better to receive this message 25 times than to receive the virus and open it.

FYI It is not a hoax. I checked it out -<http://www.snopes.com/computer/virus/postcard.asp>

If you receive a mail called" POSTCARD," even though sent to you by a friend, do not open it! Shut down your computer immediately.

This is the worst virus announced by CNN. It has been classified by Microsoft as the most destructive virus ever. This virus was discovered by McAfee yesterday, and there is no repair yet for this kind of virus. This virus simply destroys the Zero Sector of the Hard Disc, where the vital information is kept.

Check it out for yourself!

# Hoax Example (cont.)

This is a good example of a Hoax variation. They even use one of our recommended websites in their scam (snopes.com). If you follow their link you will see that the POSTCARD virus is real. Two things are amiss, however.

- One, the POSTCARD virus has been around since July 2007, hardly a surprise to anti-virus companies who update their software daily.
- Two, the POSTCARD virus doesn't "burn your hard drive". It turns it into a zombie to attack websites like eBay and CNN.

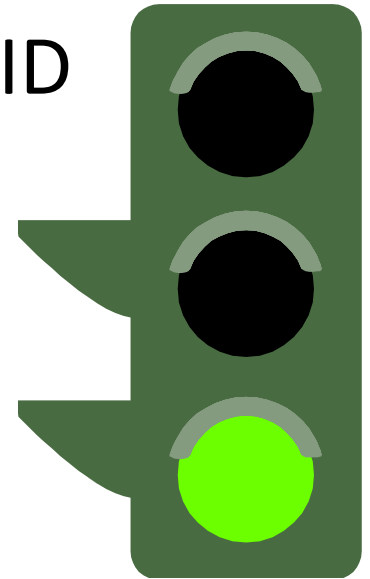
# Hoax Example (cont.)

If we type “postcard hard disk virus” into the Google search engine, the first three references concern a virus hoax called “A virtual card for you”.

If we type the search terms above into snopes.com, it brings us to the entry for “A virtual card for you” virus hoax entry. It contains the EXACT text of our email.

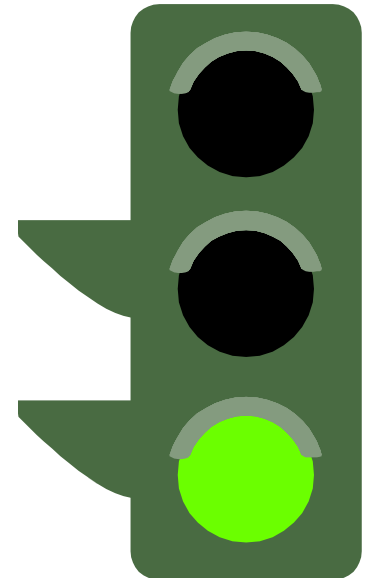
# Acceptable Use

- End Users are accountable for any violations associated with your user ID
- Use of IT infrastructure must be consistent with the goals of your organization
- All computer equipment and electronic data created by it are University property



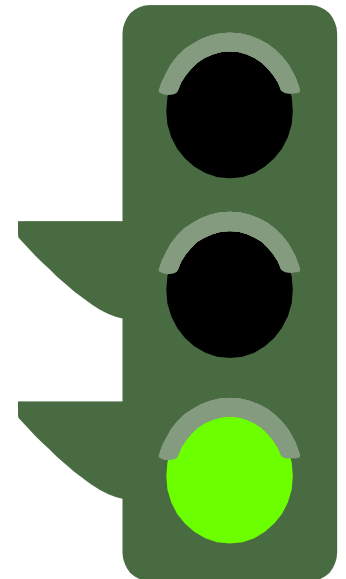
# Acceptable Use cont...

- End users must exhibit responsible behavior by complying with:
  - All Federal and State laws
  - Organizational Rules and Policies
  - Terms and computing contracts
  - Software licensing rules



# Acceptable Use Cont...

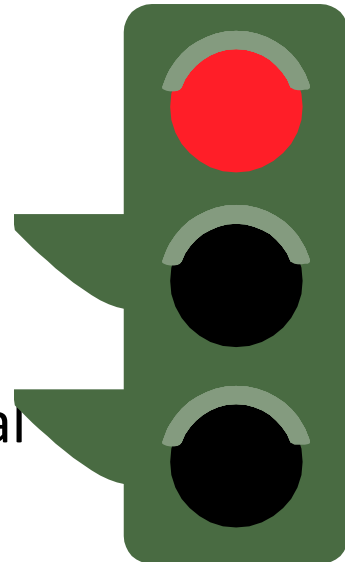
- Proper authorization must be obtained:
  - to use LSU computing resources
  - before accessing or sharing data
- Responsible for use of your assigned use ID
- Participate and cooperate with the protection of IT infrastructure
- Take reasonable precautions to avoid introducing computer viruses into the network



# Illegal Use of the I.T. infrastructure

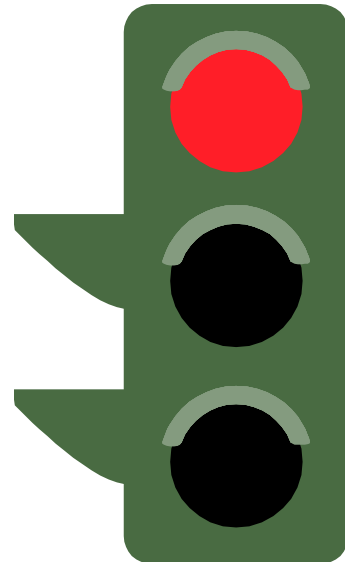
## End users shall not:

- Engage in any activity that jeopardizes the availability, performance, integrity or security of the I.T. infrastructure
- Use computing resources in a wasteful manner
- Use I.T. resources for personal gain or commercial purposes not directly related to your job
- Install, copy, or use any software in violation of licensing agreements, copyrights, or contracts



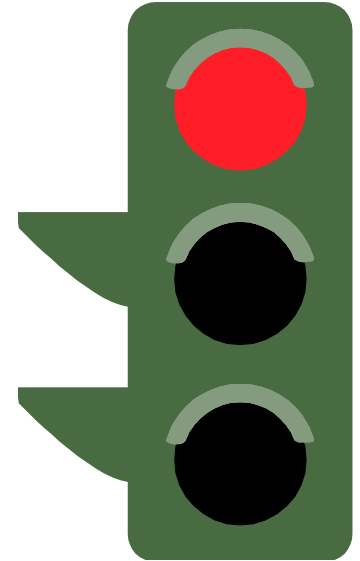
# Illegal Use cont...

- Obtain or attempt to access the files or electronic mail of others unless authorized by the owner
- Harass, intimidate, or threaten others through electronic messages
- Construct a false communication that appears to be from someone else
- Send or forward unsolicited E-mail to lists of people you do not know
- Send, forward, or reply to E-mail chain letters
- “Reply to all” to mass E-mail mailings



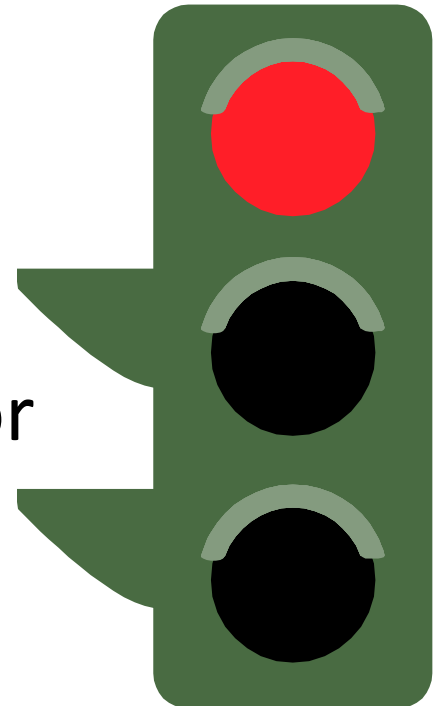
# Illegal Use Cont...

- Create or transmit any offensive, obscene, or indecent images, data, or other material
- Retransmit virus hoaxes
- **Engaging in these activities could result in disciplinary action up to and including loss of network access, termination of employment and civil or criminal liability**



# Examples of Illegal Use:

- Use of “Napster” clones (Kazaa, Morpheus, etc.)
- Playing “Internet radio or “web radio”
- Operating a website for personal use or business use not related to your job



# Social Engineering

- A hacker attempts to gain access by using non-technical means to infiltrate a computer system
- Examples of “People Hacking” include:
  - Telephone conversations from someone pretending to be a Help desk supporter
  - shoulder surfing
  - Physical access to your computer
  - Dumpster diving
  - Other impersonation
  - Incident reporting



# Telephone Conversations

- A hacker might attempt to gain your password by impersonating a Help Desk supporter during a phone conversation
- **Passwords should never be given out during a telephone conversation**
- The Help Desk will ask for a secondary form of authentication when unlocking your account or resetting your password such as:
  - Last four digits of your Social Security number
  - Date of birth
  - Place of birth

# Shoulder Surfing



- A hacker could attempt to learn your password by:
  - watching while you type your password
  - snooping around your CPU while you type it
- **Prevention:**
  - **type your password quickly or when no one else is watching**
  - **never write your password down**

# Physical Access to your computer

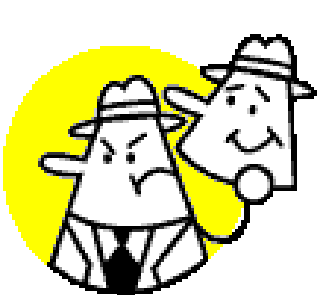


- A hacker could remove, destroy, or otherwise damage your computer
- Prevention:
  - always use good physical security measures to prevent theft or damage to your computer

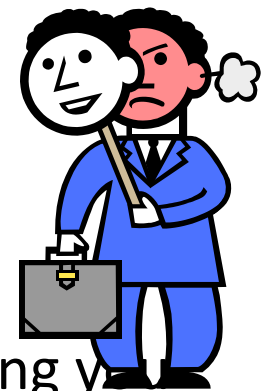


# Dumpster Diving

- A hacker might learn information by:
  - scouring trash for passwords written on scraps of paper
  - documented computing procedures
  - discarded hard drives, discs or CDs
- Destroy all information in accordance with policy once it is no longer needed
- Contact your local computer supporter or helpdesk for assistance with properly erasing or destroying computer media



# Other Impersonation



- A hacker might attempt to:
  - impersonate a member of the I.T. department by sending you a link to a fake website to glean passwords
  - distribute a fake “required” patch to you which is really a virus
- **Prevention:**
  - make sure that you have antivirus software installed on your computer
  - never share your password
  - call the help desk or your computer supporter to verify instructions

# Incident Reporting



- Notify your local computer supporter or helpdesk if:
  - You suspect your password has been compromised
  - You suspect your files have been tampered with
  - Your computer behaves abnormally
  - You suspect someone has obtained or is trying to obtain unauthorized access

# Confidentiality/Safeguards

- Extra precautions must be taken when protected information (health or financial information) is stored on a local computer:

- » Data must be stored using encryption in case laptop is lost or stolen
- » Lock your computer if you leave your machine unattended
- » Written backup and disaster plans must be in place



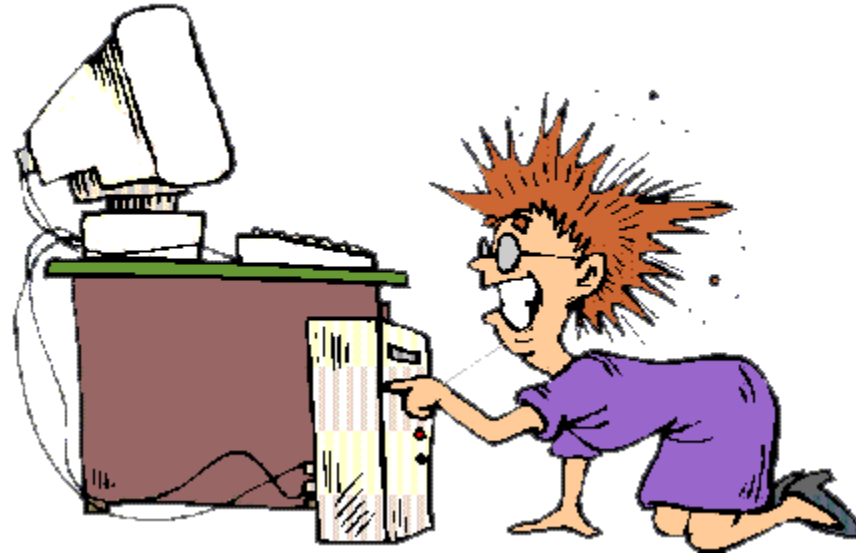
# Confidentiality/Safeguards

- Extra precautions must be taken when accessing protected information (employee, student, health, financial, etc.) from a remote location.
  - Make sure your connection is secure by using a VPN (Virtual Private Network) or SSL (little lock icon at the bottom of your browser screen)
  - When accessing email or other files via the World Wide Web from a computer at a hotel business center or conference:
    - Don't allow anyone to read your screen over your shoulder
    - Make sure any copies of such files are deleted from the Internet cache on the computer before you leave
  - When working from home, ensure the computer you are using has up-to-date virus software and operating system patches

# Why should I take these precautions if I only use my PC for reading email ?

- The reason:
  - Hackers use a technique called “**Escalating Privilege**” which enables them to turn ANY user account into an administrator account. All they need is an account to get past the firewall

**Make sure you follow LSUHSC-N.O.'s  
procedures or you may end up like  
this...**



# **Questions?**

## **We Are Here to Help!**

Office of Compliance Programs

433 Bolivar St.

Suite 807

New Orleans, LA. 70112

568-2350