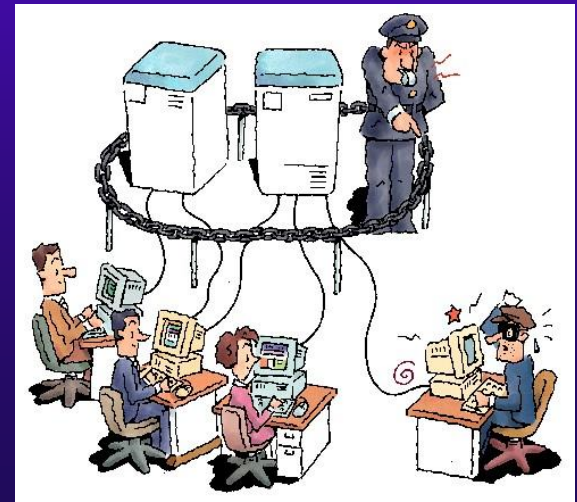




**Protecting Student, Faculty
and Staff Information
Requires You!**

Protect Student, Faculty, Staff Personal Information against:

- ◆ **Hackers** – Do not store sensitive information (SSN, Credit Card numbers) on your hard drive.
- ◆ **Inappropriate Disclosure** – Follow proper procedures and government regulations to ensure records are kept confidential.
- ◆ **Lost Data** – Always backup records so that important information is available when requested.
- ◆ **Inaccurate Data** – Develop valid data entry procedures and control access to files.





YOU are the KEY

The single biggest security risk is Your Password.

- *Cracking passwords is still the most frequently used method of attack.*
- *Hackers now have a lot of computing horsepower to carry out “brute force” attacks (i.e. systematically guessing thousands of likely passwords).*
- *There are also widely available cracking “dictionaries” that allow automated attacks covering every English word, and then some, in a matter of a few hours.*

For this reason, “strong” passwords are recommended. A “strong” password will not be based on any common word (Including proper nouns), will be a minimum of six characters long and will contain uppercase and lowercase letters, numbers and punctuation marks.

YOU are the KEY

You can prevent unauthorized access to your computer by:

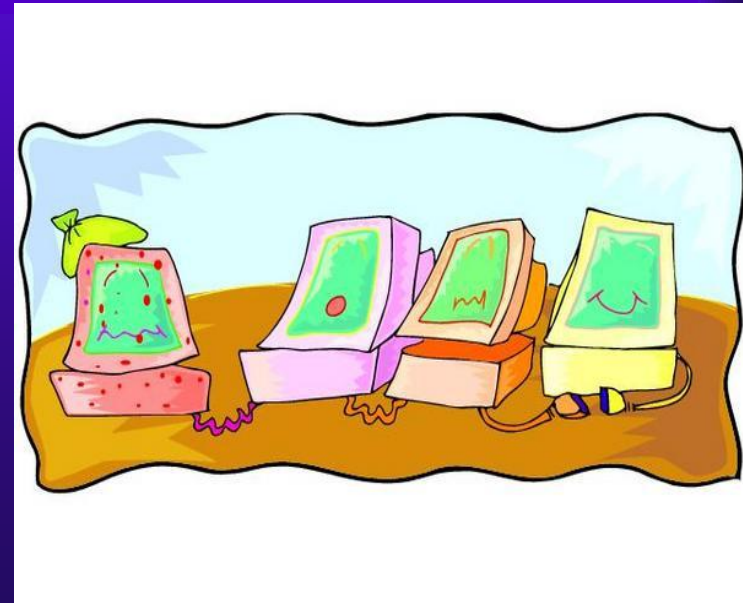
- *Changing your passwords often*
- *Not sharing your passwords with others*
- *Making sure your password is strong*



YOU are the KEY

- ◆ You ensure the network is protected by:
 - Updating your virus protection software
 - Updating your operating system software

It is critically important that your own computer has anti virus software installed, and that you update it regularly—weekly, at the very least. Maintaining strong protection against viruses and other malware does not guarantee your computer will never be compromised, but it is one of the single most important steps you can take.



YOU are the KEY

You ensure university data is secure and accurate by:

- ◆ Ensuring that data is entered correctly.
- ◆ Turning off the computer each night.
- ◆ Not accepting emails from unknown sources.
- ◆ Not visiting or doing business with web sites that are not secure.
- ◆ Installing a personal firewall.



Anti-virus software, regular operating system updates and personal firewalls provide excellent protection from most threats when used together. We recommend using a personal firewall (hardware version) when you are storing personal financial information on your computer (SSN, student ID numbers, credit card numbers, etc.)

YOU are the KEY

- ◆ You protect the university by:
 - Ensuring that you have a license for all the software on your computer.

Weber State University does not permit, tolerate or condone the unauthorized copying of licensed commercial materials by staff, faculty or students. Any individual engaged in unauthorized copying or use may face disciplinary proceedings, civil suits, criminal charges, penalties and fines.





**New Government
Regulations Designed
to Protect Information**



New Government Regulations

- ◆ **Gramm-Leach-Bliley Act**...privacy of consumer financial information
- ◆ **Sarbanes-Oxley**...Financial integrity and safeguarding of assets
- ◆ **FERPA**...privacy of student information




Gramm-Leach-Bliley (GLB)

- ◆ This act requires special steps to protect SSN, Credit Card numbers or other personal financial information.
- ◆ This act also requires that we train our employees on how to manage their personal computers responsibly.



Sarbanes-Oxley (SOX)

- ◆ This regulation requires that the financial information of the institution is accurate.
- ◆ This regulation requires that that all student information is accurate.
- ◆ This act requires processes to report inappropriate activities. At Weber this can be done by calling 801-626-TIPS



Family Educational Rights and Privacy Act (FERPA)

- ◆ This regulation limits who can get student information.
- ◆ It limits how we can give information (telephone, in person or fax).
- ◆ It also requires training for those who deal regularly with student information.



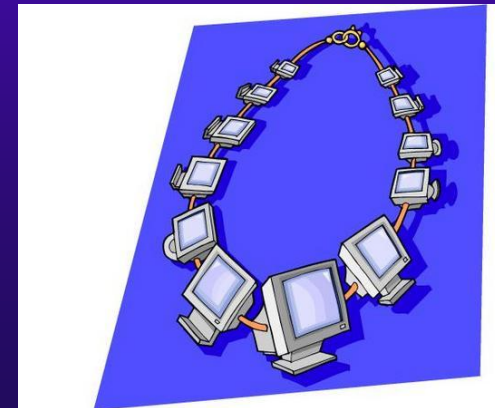
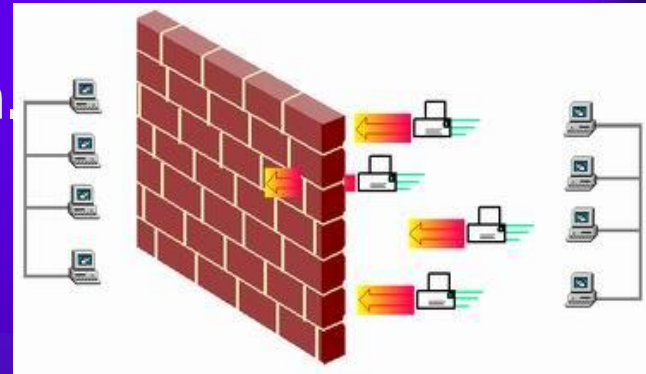
Weber State University Policies and Procedures Designed to Protect Information

These policies and procedures include:

- ◆ **Protection for Servers**
- ◆ **Protection for Applications (Lynx/Banner)**
- ◆ **Protection for Personal Computers**

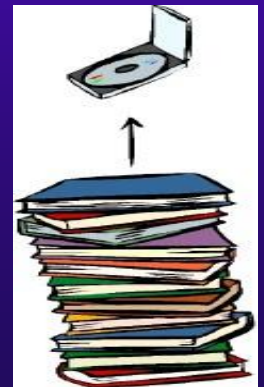
Protection for Servers

- ◆ IT ensures that all servers have firewalls to limit the ability of hackers to access our system.
- ◆ IT uses Intrusion Detection Software to identify intrusion attempts.
- ◆ IT ensures that the servers have adequate disk space to store the information.
- ◆ IT ensures we have the ability to recover from system & network failures.



Protection for Applications (Lynx/Banner)

- ◆ **Access is limited by:**
 - Specific job requirements
 - Data custodian approval
 - Required written approval
 - Training requirements
- ◆ **The system has password controls.**
 - Required password changes
 - Required strong passwords
 - Users are locked out after 3 failed logins
- ◆ **Backups are prepared so that the information can be recovered from data base failures.**
- ◆ **Important reports and information are archived**



Protection for Personal Computers

- ◆ Your actions can undermine network and application controls.
- ◆ Information can be accessed inappropriately through your personal computer by:
 - Weak passwords, not changing passwords or not keeping them confidential.
 - Leaving your computer on overnight.
 - Virus software and operating systems that are not updated.
 - Storing sensitive information on your hard drive.





Internal Audit is in the Miller Administration Building

- Room 214 -

1018 University Circle - Ogden, Utah 84408-1018

or Call: 626-7160