LSU Health Sciences Center

LSU Health Sciences Center Office of Computer Services

Bettina Owens

Assistant Vice Chancellor

Information Technology

LSU Health Sciences Center

LSUHSC New Orleans IT

PC and LAN Supporters

- Provide IT services that are specific to the school or division.

- School of Medicine
- School of Dentistry
- School of Nursing
- School of Allied Health Professions
- School of Public Health
- School of Graduate Studies / Academic Affairs
- Administration and Finance

Office of Computer Services

- Provides IT services that are used by everyone.

LSU Health Sciences Center

OCS Services

Audio Visual/Videoconferencing/Access Grid
Help Desk / Backups – backup 500 TB
Database Services - 451 Databases on 50 Database Servers
Networking – LSUHSC NO and LSU HCSD – 60 Sites, 2 Datacenters
Internet 1, Internet II, LONI (LamdaRail), LaNET
Applications and Special Projects – 140 applications (PeopleSoft, Moodle, Budget, Card Access, …)
Server Support – 520 Servers and 72 TB of Data Storage
Telecommunications - > 2,900 Telephones and 1,298 Mobile Devices
Web / Email – 120 Websites, 51 Web and Email Servers, and 16 Digital Signs
Block 22,222,928 SPAM Email Messages a Month (1/3 of all email received)
Enterprise Security - 25,173 User Accounts (NO, SH, HCSD), Firewalls, VPN, IDS, Wireless and Port Authentication, Access Control, and Disk Encryption
141 hits a second on our firewalls

LSU Health Sciences Center

IT Challenges

1. Data Growth on Servers and Backups
2. IT Security
3. Internet Usage
4. Mobile Devices

LSU Health Sciences Center

How Do we Manage Data Growth on Servers and Backups?

1. Monitor Servers for Non-University Related Data.
   - If images, music, videos, or other large files are placed on the file servers, the PC supporter is asked to work with the end user to determine the nature of the data and to remove it if it is personal.
2. File Archiving
3. Email Archiving

LSU Health Sciences Center

Challenge Two: IT Security

- Goal
  - Provide an IT infrastructure that ensures
    - Confidentiality
    - Integrity
    - Availability
- How Do We Obtain This Goal?
  1. IT Security Policy
  2. Protection Against Threats
  3. Safeguard Protected and Restricted Data
  4. Restrict Internet Use

LSU Health Sciences Center

IT Security Policy

- CM 42 Information Technology Infrastructure Acceptable Use
  - http://www.lsuhsc.edu/no/administration/cm/cm-42.aspx
- Points To Remember
  - Don't send, forward, or reply to chain emails
  - Don't "reply to all" to a mass email
  - Don't use the LSUHSC IT infrastructure for personal gain
  - Don't install FTP servers or web servers without IT consultation
  - Don't share your user ID and password
  - Log off of any computer when you leave the area
  - Don't install, copy, or use any software in violation of licensing agreements, copyrights, or contracts
  - Don't waste LSUHSC IT resources (email backgrounds, computer games, web radio, music videos, web television, …)
  - Don't respond to phishing emails (your user ID will be disabled if you respond to a phishing email)

LSU Health Sciences Center

Phishing

- **From: Commons, Judith K [mailto:jcommons@saclink.csus.edu]**
  Sent: Thursday, July 28, 2011 9:52 AM
  To: Undisclosed recipients
  Subject: ITS Alert: Information Regardng Network
-
- Please forward this message to all staff/students:
-
  In order to finalize the network replacement work we unfortunately need to reboot the core network equipment to clear out artifacts introduced by the installation process.
-
  Please you are to re-login below so that you will not have any login problem after the core network has been reboot.
-
  http://cbess-webapp2.host-ed.net/secureauth/cddxg6FDS8Nf2/submit1.php
-
  Please consider all services to be at risk with some disruption.
-
  We will be working hard to ensure all disrupted services are returned as soon as possible.
  We apologies for the short notice, disruption and inconvenience that this will cause.
-
  - The IT HelpDesk Team

LSU Health Sciences Center

What Can Someone Do With Our User ID and Password?

- The actions of one person revealing their user ID and password threatens other innocent members of LSUHSC and may subject them to identity theft.
- Identity thieves may rent an apartment, obtain a credit card, or establish a telephone account in your name.
- Victims are cheated out of thousands of dollars and spend months repairing damage to their good name and credit record.
- Consumers victimized by identity theft may lose out on job opportunities, or be denied loans for education, housing, or cars because of negative information on their credit reports.
- In rare cases, people may even be arrested for crimes they did not commit.

LSU Health Sciences Center

Identity Theft - Why Should We Care?

- Federal and state laws and regulations are intended to protect the privacy of patient, student, and employee records.
  - The exposure of private confidential data can cost millions in fines and damages. Such exposures could also severely harm the reputation of LSUHSC.
- The FTC estimates that as many as 9 million Americans have their identities stolen each year.

LSU Health Sciences Center

Protected Data

- Protected Data - information that shall have extraordinary controls over its use and disclosure due to the sensitivity of its content. Unauthorized use and disclosure can lead to personal, reputational, and/or financial damage to employees, students, and/or patients.
  - Examples of Protected Information include, but are not limited to:
    - » employment records, medical records, student records,
    - » personal financial records (or other individually identifiable information),
    - » research data,
    - » trade secret information and
    - » classified government information

LSU Health Sciences Center

Restricted Data

- Restricted Data - information of such a sensitive nature that access is limited to those individuals designated by management as having a need to know.
  - Examples of restricted information include but are not limited to:
    - ongoing investigation files,
    - pending litigations files,
    - attorney-client privilege emails and files,
    - files subject to litigation holds,
    - psychotherapy notes, and
    - files regarding disciplinary action
  - Use encryption on any protected or restricted data on a mobile device that leaves the university.
  - Don’t send protected or restricted data in email.

LSU Health Sciences Center

A Few Ways to Protect Against IT Security Threats?

- Use anti-virus and anti-spyware to block viruses, Trojans, worms, and malware.
- Use McAfee's SiteAdvisor software to display a green check next to safe sites in a search list.
- Install up-to-date operating system patches
- Monitor the network with intrusion detection systems to guard against the spread of computer viruses, Trojans, worms, and other various malware attempts.

LSU Health Sciences Center

How Can We Safeguard Protected and Restricted Computer Data?

- Use Strong Passwords
- Provide access to data only to those who need it to do their job
- Encrypt protected or restricted data
- Use a password protected screen saver and lock your computer when you walk away
- De-provision staff and faculty accounts immediately upon leaving the university and students 60 days after graduation.

LSU Health Sciences Center

Challenge Three: Internet Usage

- LSUHSC-NO Internet Network bandwidth is limited. Faculty, staff, and students depend on availability of Internet access for:
  - Access to student learning and training videos
  - Telemedicine / videoconferences
  - Research
  - Access to applications
  - High-speed data and image exchange
  - Collaborative initiatives
  - Purchasing
  - Software downloads
  - …

LSU Health Sciences Center

How Do We Ensure Internet Availability?

- Many websites are blocked from use
  - If you cannot get to a web site that you think is wrongly blocked, contact security@lsuhsc.edu to see if it is blocked and to have it unblocked.
- Network Abuse Application
  - Monitors for unusual network activity
  - Documents high bandwidth usage
  - Generates weekly lists of the top users of Internet bandwidth
    - Reports are reviewed to determine if the bandwidth used is primarily university related
- If the bulk of a user's usage is deemed non-university related, it is reported to the user's Dean/Vice Chancellor
  - A user that shows up on the Network Abuse List three times has his/her network access disabled.
    - Approval of the Dean/Vice Chancellor and the Vice Chancellor of Administration and Finance is required to re-enable the network access.
    - A user may also be restricted to the white list once access is reinstated.

LSU Health Sciences Center

Ways to Show Up on the Network Abuse Top User's List

- Leave your Internet browser open to a page like msn.com that cycles through videos
- Listen to streaming radio.
- Watch music videos, sports videos, political videos, religious videos, …
- Watch non-business/school Youtube videos.
- Download wedding or other photographs.
- Watch Netflix movies on your mobile device while it is connected to the wireless network.

LSU Health Sciences Center

Challenge Four: Mobile Devices

iPhones, iPads, Androids, Blackberry Devices, …

- Mobile devices are everywhere.
- Risks
  - The portability of a mobile device makes it more likely to be lost or stolen.
  - If a mobile device does not have a passcode set, anyone can pick up the device and read email that may contain protected or restricted content.

LSU Health Sciences Center

Mobile Devices

iPhones, iPads, Androids, Blackberry Devices, Windows Mobile, …

- OIT IT Policy 1-24 on the use of smartphone devices when accessing state networks and to protect against phone hacking and access to sensitive data states:
  - "Smartphone devices that are used to access state email and/or networks, but not including devices that only access email through a web-based interface, must have the following security measures enabled: a minimum of a 4 digit PIN is required to access the device; a Group Policy or setting that is pushed down from the email server or wireless enterprise server, which after ten failed login attempts to the device will initiate a complete data wipe ensuring all state data is removed.
  - This policy applies to both state-owned devices and privately-owned devices that are used to access data owned by the state, including email."

LSU Health Sciences Center

Mobile Devices

iPhones, iPads, Androids, Blackberry Devices, Windows Mobile, …

- LSUHSC will implement the OIT IT Policy 1-24 on the use of smartphone devices in the near future. You will receive a mass email explaining the process and the date.
- In the interim, please remember that you are responsible for guarding all LSUHSC protected and restricted data that resides on your mobile device.
- The best mechanism to protect your data and to deter hacking is to:
  - Set a passcode on your mobile device.
  - Have a strong LSUHSC network password.
  - Be cautious about the software you download to your mobile device.

LSU Health Sciences Center

Social Networking

- Facebook usage is not currently allowed from the LSUHSC NO campus network.
- Justification for university use is reviewed and allowed if deemed appropriate.
- When using social networks off campus for personal use it is advisable to use a personal email.
- When participating in or posting content on any site from LSUHSC using LSUHSC credentials, it is good practice to engage in appropriate use.
  - For example, LSUHSC colleagues should not use social media for unapproved marketing or public relations and one should always follow the LSUHSC code of conduct and the CM-42 computer usage policy.