This October, for Cyber-Security Month, UITS is emphasizing security for mobile computing devices. Mobile computing has expanded significantly from the days of laptops. Smart phones and handheld tablets, like iPad, have emerged on the computing scene en masse.

As these types of devices grow in numbers from an obscure few to numbers rendering them as commonplace, so too, do their risks. To date the number one risk is the lack of understanding how such devices provide a gateway to personal and University data, and the steps prudent to protect that data.

The most common smartphone/tablet interface into University services is through the Exchange e-mail system. As with any device which connects to an IU system, protection of that access becomes prudent by policy.

The three main risks to mobile computing devices are: Loss of the device and access by unauthorized individuals. Compromise by installing malicious applications. Other forms of device hacking, such as through the very susceptible Bluetooth connection.

The following are a few simple steps that can be taken to safeguard the device and data.

**Set a Passcode Lock**

Access to the device should not be allowed from power on or wake up from sleep mode, until a passcode is entered. While most default passcodes are a 4 digit number, a determined thief is likely to eventually break such a simple code. Many devices include advanced settings which allow a person to use more than 4 digits, or even to use a passphrase utilizing letters as well.

Many devices also allow you to set an auto-wipe after a set number of failed attempts to enter a passcode. This would prevent data access from a determined thief who will keep trying passcodes until they find yours.

**Enable Automatic Sleep Mode**

Enabling sleep mode helps prevent data exposure on a misplaced device, instant access to your email account, and invokes the passcode requirement for access. Remember, if you don’t have to do anything special to access your data or email from your mobile device, neither would a thief.

**Enable Remote Wipe**

This step allows for the possibility to remotely wipe the device should it end up lost or stolen. Several methods are available for this, including through the University’s Exchange email system if the device has been used to access IU Exchange email from the device prior. Wiping the device should also be performed when the device is being retired, replaced by a new device, or sold/ transferred to another party.

**Data Encryption**

Many devices have the ability to turn on data encryption. Encryption prevents someone from accessing data that may be stored in the device memory or on expansion cards, if the encryption utility is configured properly.

**Disable Bluetooth**

Hacking in to your device via the Bluetooth connection is a trivial matter for a knowledgeable hacker. Disable Bluetooth completely if you do not use it, otherwise, only enable Bluetooth when you will use it.

**Other tips include:**

* Protect your phone and voice-mail passcodes and never leave confidential information in voice-mail or text messages.
* Be wary of text messages, system messages, or events on your device that you did not ask for, initiate or expect.
* Keep confidential or private data off the device.
* Only download apps from trusted sources or the official app market to prevent viruses.
* Note the permissions an app is asking for. (Why would a game or traffic app need to access your contacts or messaging?)
* Keep watch over your battery levels. If they take a huge dive when you’re not using the phone, say overnight, it indicates that there’s some sort of activity (downloading/uploading?) taking place during that time.

---

**Highlights of this issue:**

- From the Desk of . . . . . . . . . . . . Page 2
- Familiar Faces in New Places. . . Page 2
- Meet the Staff . . . . . . . . . . . . . . Page 3
- Updates and Upgrades. . . . . . . . . Page 4

Edited by: Kathleen Weidner
Joel B. Langston
Dear Campus Community,

The 21st century has marked the emergence of a new era, as the industrial economy is replaced by an information economy. Never before has so much information been available on such a global scale. Access to systems and data can occur at light speed from most anywhere on the planet. The complexities of the information revolution are seemingly overshadowed only by the sheer number of innovations which has led to this pinnacle point in time when one can literally hold, and access the whole world in the palm of their hand.

From each new form of computing innovation comes a unique set of challenges for information security officers who are charged with ensuring infrastructure security and data privacy.

With the emergence of innovation, the mantra “data access at anytime from anywhere” is a reality. It is increasingly important to guard access to your credentials and to understand the appropriate use, security, and storage of data, especially data that contains sensitive information.

In the interest of protecting University data, University reputation, and your own financial accounts, please take advantage of emerging security-related communications from UITS. To learn more visit the UITS Security web site at http://uits.iu.edu/page/amef. I am also always available to meet with people individually or as a group, to discuss information security and privacy.

Best Regards,

Bruce Bryner
Information Security Officer

Familiar Faces in New Places

Over the summer, Media Services (IMS) and UITS combined services to leverage the audio/visual, media production, and classroom technology expertise of the talented professionals in both organizations.

Jim Yocom is now Director of Instructional Media Services and Communications. In this role he will report to CIO Beth Van Gordon and will continue to direct Media Services as well as Classroom Technology Services. Kathleen Weidner has become IT Project Manager and Communications Officer, and has moved to the IMS office area on the ground floor of Northside Hall. Jason Sykes has become Manager of Classroom Technology Services, and has moved to the CTS offices in Wiekamp Hall. Joel B. Langston is now Manager of Media Services.

In the short term, processes to request services will remain unchanged. In the long term, support and services will be enhanced as the teams leverage each other and the strengths of all IU campuses’ information technology professionals.

Jim Yocom has moved from his office at Northside 075A to 075B.
Kathleen Weidner has moved from her office in Wiekamp to Northside 075A.
Jason Sykes has moved from Northside to Wiekamp 1145A.
Joel B. Langston is still located in Northside 037A.
Meet the staff....

Sue Baker is the Consultant Supervisor for the IU South Bend Student Technology Centers. She hires, trains, and schedules the lab consultants to cover the campus labs. Sue arranges lab reservations for special classes as requested by faculty and staff.

Here are her responses to our get-to-know-the-staff questions:

**What do you like about working in IT at IU South Bend?** I love the interactions I have with the students, faculty and staff members (especially our international friends). There are different challenges every day; so, I don’t get bored.

**What brought you to IU South Bend?** I started working here part-time while completing my nursing degree.

**What do you like to do in your free time (hobbies, interests)?** Family, travel and gardening.

**Can you tell us something about yourself that might surprise others?** I have twin sons.

Computing changes in the Schurz Library

UITS, working with the Library and Facilities, is planning to provide an additional 36 computers on the 2nd, 3rd, and 4th floors of the library in the Spring semester. New computer desk units, similar to those in the Information Commons, will replace the existing large round tables in the center of each floor. Printers which can be accessed by students using the computer clusters or their own wireless laptops will be located nearby.

Current second floor setup

See the picture above showing the proposed layout for each floor. This project is expected to be completed during spring break in March 2012.

*Newsletter archive at:* [http://it.iusb.edu/newsletter.shtml](http://it.iusb.edu/newsletter.shtml)
**Did you know?**

**WCMS Migration**

Things are moving along as we gear up for migrating web sites into the Web Content Management System (WCMS). In early October we had 55 people attend a town hall meeting. This was the first town hall meeting that was open to the entire campus as the previous ones were meant for web account sponsors. A number of questions were asked ranging from accounts to workflows. Be sure to join us for the next town hall in November. Look for an announcement on the bulletin board.

**Wireless**

This year one of the Information Technologies projects has been to upgrade the wireless access throughout the campus. The upgrade consisted of installing a newest HP wireless access point along with controller cards. Since then, more than 90 access points have been installed. Northside Hall is currently getting the new units which are replacing older access points and new ones installed in weak areas. This is the last IUSB Building to be upgraded. The Purdue Building will be upgraded early next spring. If you encounter a dead spot in any building please report it to the IT Support Center.

**Wiekamp 1001**

The technology upgrade to Wiekamp 1001 is well under way. A new 6,000 lumen projector offers brighter and more vivid images with full high definition resolution. The dual-lamp system will automatically switch to a spare bulb in the event of failure. The new JBL speakers and Crown amplifier offers an enhanced listener experience for both program sound and microphone support. Watch for more upgrades as the year progresses.

**NEWSFLASH**

The equipment in Northside 075B has recently moved into room 037. Check your schedule to make sure which room you’ve booked.

**Updates and Upgrades ...**

**New Procedure for Videoconference Requests**

IMS is streamlining the way requests are submitted for using the videoconference rooms on campus. Instead of calling and asking to see if a room is available, you are now able to see and schedule for yourself. The Virtual Indiana Classroom Operations (VICOPS) in Bloomington has a useful website to show how to use the Outlook Calendars when requesting rooms.

http://www.indiana.edu/~video/vidcon/schedule_outlook.php

Here in South Bend the rooms are labeled as...

Sb-N038  Sb-N072  Sb-N037

Once you have scheduled a videoconference room, you may be interested in booking a video bridge or creating your very own, personalized, video bridge you can share with your colleagues. No need to wait for the Outlook calendar video bridges to become available. You can have your videoconference when you want it!

The IU Knowledge Base has the answers.

http://kb.iu.edu/data/ause.html

As always, if you have questions feel free to contact Joe Haase in IMS at 520-5558 or jhaase1@iusb.edu.

**My Favorites ...**

**Top 5 (iOS) Apps from UITS staffer Joel B. Langston**

1. **Instagram**
   This app is a mashup of Facebook and Flickr, you take photos, add a caption, tweak it a little with some great filters and upload to the web. People follow you who like your photos or are friends. Personally I’d rather see a photo of what you’re up to than your Facebook update.

2. **Find iPhone**
   This is one of my favorite, but least used apps. It’s a great security blanket app. If I ever lose my phone, I can use my iPad or the web to find it. I can tell my phone to erase itself remotely if it’s been stolen or I can make an alarm go off to help me find it under a mountain of clutter.

3. **Yelp**
   This is a social app for finding cool places around you. Recently found a Thai restaurant nearby that was great, thanks to Yelp. You can rate places you go and help others find that one cool store they’d never find on their own.

4. **Penultimate (iPad only)**
   This app is for use with a stylus for taking notes or making simple drawings and charts. It has completely replaced a legal notepad for me. Hundreds of pages of notes all stored on my iPad and backed up on my computer. Love it.

5. **Music Mine (iPad only)**
   This app is for people who want to discover new and interesting music. There is a great public radio station in Santa Monica, California called KCRW. They are always playing something amazing. Every day their DJs upload songs, videos, commentary and bios to this app. Make no mistake, this is not an app where you can go back and hear a song that you liked a week ago, by that time all the music has been replaced by the newest of the new.