This spring, most Indiana counties will observe Daylight Savings Time (DST) for the first time since 1970. In 2006, DST begins at 2 a.m. on the first Sunday in April (April 2) and ends at 2 a.m. on the last Sunday in October (October 29).

Because of modifications to GroupWise, to accommodate the change to Daylight Savings Time, your calendar items scheduled between April 2 at 2:00 a.m. and October 29 at 2:00 a.m. are now showing up an hour later than originally scheduled. Unfortunately, this problem was unavoidable as we adjusted the system to recognize Daylight Savings time. The only way to correct this problem is to manually change your appointments back one hour. We do apologize for the inconvenience this has caused and appreciate your patience and understanding. Similar problems are being experienced by other institutions in Indiana that use electronic calendars.

IT Services has implemented a change on the GroupWise e-mail server which has modified the time zone to “Eastern Time (GMT –05:00).”

(Continued on page 3)

Data Security and Your Workstation

With recent security incidents at other campuses and businesses, it has become imperative that we all take steps to protect data accessed through our computers. Precautions should also be taken to protect data stored on any portable devices such as laptops, disks or flash drives. Here are a few key steps that we can all do quickly to increase security significantly.

Your cooperation is key to providing overall campus data security!

First Line of Defense

Use the password protected screen saver. Window users: when your workstation is going to be unattended, initiate the password protected screen saver as you leave, rather than wait for it to pop up on its own. To do this, either press Ctrl +Alt+Del to bring up the panel which allows you to Lock the workstation or press the Windows icon key and the L key to lock it immediately. Mac users: the control panel provides an option to set up a password protected screen saver.

When you leave the office for the day, please restart, power down or logoff via your operating system shutdown options. This simple step provides some protection against unauthorized use of your workstation. Selecting the restart or power down option involves a reboot which refreshes your workstation, and the next time you log in to the network, the Trend OfficeScan antivirus software installed on your Windows workstation automatically updates.

Keep your workstation up-to-date with vendor patches and virus protection by activating updates promptly when you are signaled that they are ready. Windows XP/2000 users: when you see the “msg” at the bottom of your tool bar that says you have new updates, please click on the button and add your updates. Mac users: Click on the Apple icon, select Software Updates and set up the function to automatically install the updates.

Don't Collect it or Store It

If you don't need private information such as social security number, financial or medical information, or even full name, then don't collect it and don't store it on any of your directories, including the I: or O: drives. In Banner, use PIDM to uniquely identify students instead of SSN when appropriate.

Protect the Data

If some private information must be collected, save the file as encrypted, and password protect it. Most applications, including Brio and Excel, typically provide these options in the Save As > Tools options. If your department has a Microsoft Access database, this data can also be secured by the creator of that database.

Avoid Sending Sensitive Data Through Email

Sensitive data should not be sent via email, especially off-campus. For departments where this is unavoidable, encrypt and password protect the data as described above.
Periodically IT Services receives patches and updates from our network and operating system vendors that are vital to the security and function of the IPFW network and your desktop. When these patches and updates are distributed, it is critical that you apply them to your workstation in a timely manner. To assist in that goal IT Services has implemented a PatchLink process. The PatchLink process will distribute the patch or update to your workstation to be automatically installed.

Some important notes on how patches may be applied:

- If a restart (reboot) of your computer is necessary to fully implement the patch or update, a prompt will display asking if you want your workstation to restart now. You do have the option to restart at a later time; however it is very important that you do so at the end of business that day.

- Occasionally you may see an option when shutting down your computer which states “Install Updates and Shutdown.” If you should see this option, select it instead of “Shutdown.” Use this option to help make your computer more secure before you turn it on again. With this option, Windows will install the updates and then automatically shut down your computer. Note: No one else can use the computer while the updates are being installed.

Important! Do not turn off or unplug your computer while updates are being installed. If you interrupt the update process—during shutdown only—you could damage files that Windows needs to operate. This option appears only if you are running Microsoft Windows XP Service Pack 2 (SP2) and you turn on Automatic Updates from the following URL:


Since updates and patches are frequently distributed by the vendors, this process will be ongoing. This system will work in conjunction with Windows updates that are automatically distributed by Microsoft. If you regularly apply Windows updates as you are notified, PatchLink will not need to distribute those same updates to your workstation.

### Key Concepts

This column is devoted to providing our readers with time-saving techniques and short-cuts that will amaze and delight.

<table>
<thead>
<tr>
<th>Short Cut</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows + L:</td>
<td>Screensaver lock</td>
</tr>
<tr>
<td>Windows + M:</td>
<td>Minimize all windows</td>
</tr>
<tr>
<td>Windows + E:</td>
<td>Open Windows Explorer</td>
</tr>
<tr>
<td>Shift + Tab:</td>
<td>Tab backwards to the previous field</td>
</tr>
<tr>
<td>Ctrl + Shift + End</td>
<td>Highlights everything on a page</td>
</tr>
<tr>
<td></td>
<td>from the cursor to the end.</td>
</tr>
<tr>
<td>Triple Click</td>
<td>Highlights an entire paragraph</td>
</tr>
</tbody>
</table>

Would you prefer to receive your copy of INFOShare as an e-mail attachment or via campus mail in the print version? Let us know your thoughts. E-mail Pam Zepp at zeppp@ipfw.edu.

---

GroupWise Messenger Update

If you use GroupWise messenger and are prompted that a new version is available, please respond “yes” to install the update. Some significant new features have been included and are described below.

- Chat Rooms - You can create and join chat rooms, which allows several users to discuss a topic without leaving their workstations.
- Personal History - Track messages that you have sent or received. This is especially helpful when you need to find information from a message or chat room.
- Custom Online Status - Create a custom message that tells others you are online.

If you are considering using GroupWise Messenger for the first time, it’s easily installed. Simply click Start > IPFW Icons > Email > Installs. For details on these and other features, click on the GroupWise Messenger Help menu.
Use IPFW Portal For Reliable Password Synchronization

Have you ever considered how many systems require your IPFW user name and password each day? Even if you only log into your computer and e-mail, they represent two entirely different systems requiring password synchronization. Add a few more systems such as Helmke Library or WebCT resources and the complexity of synchronizing all those systems boggles the mind. As the day approaches for your password to expire, (your password expires every 182 days), remember to change your password through my.ipfw portal. Although you may see a warning at a logon prompt when starting your computer saying that your password has expired, do not change your password at this location. Just click “No” when told that your password is expiring and log in to the network. You can then open a browser, head to http://my.ipfw.edu and click on “change password.”

Change Your Password at http://my.ipfw

1. Log into http://my.IPFW with your current password.
2. Click Personal Info.
3. Click Change Password and read the requirements.
4. Enter the old password.
5. Carefully input your new password in the two remaining fields for new password and confirm password.
6. Click the Process My Request button.
7. If you are not prompted that your password has been changed, please call the Help Desk.
8. If your password has expired and you have run out of grace logins, please call the Help Desk at (260) 481-6030 to have your number of grace logins increased.
9. All IPFW network passwords expire every 185 days.

Coming This Summer

IT Services is looking at various methods to better protect networked workstations and IPFW accounts, including stronger password requirements, more frequent password changes and the possibility of turning on the Windows firewall. When we installed Windows XP Service Pack 2, the Windows firewall was turned off. We will be testing various firewall options to see what causes less disruption to our campus computing environment while at the same time providing greater security for your workstation.

Daylight Savings Time (Continued from page 1)

- All networked, campus-wide workstation clocks were automatically changed by ITS to reflect the new time zone setting.
- Appointments created prior to March 11 which appear in your calendar anytime between April 2 and October 29 will be 1 hour off.
- Appointments created after March 11 will not have this issue.

The following steps should be taken in order to correct the DST discrepancy.

- We recommend that you print a hard copy of your calendar from April through October to avoid confusion.
- Note: you can only change appointments that you posted or sent.
- Single-occurrence meetings and posted appointments created prior to 03-11-06, may be dragged back by one hour.
- Recurring meetings and posted appointments created prior to 03-11-06, should be deleted and re-created. (If you have only a few instances of recurring appointments, each instance can be dragged up to the correct time. Unlike the single appointment, dragging recurring appointments will only move that one appointment.)
- The Resend option does not work on recurring appointments affected by DST.
- For complete instructions visit the following Web page:
  http://www.its.ipfw.edu/helpdesk/dst.shtml

IT Services Help Desk is available to answer questions you might have regarding these changes. Call 481-6030 or visit the Help Desk in Kettler Hall 206.
Macromedia Dreamweaver 8 Basics  
*Thursday, 03/23/06, 10:00 - noon*

Macromedia Dreamweaver Layers & CSS  
*Tuesday, 03/28/06, 10:00 - noon*

MS Access Basics  
*Wednesday, 03/22/06, 3:00 - 4:30 p.m.*

*Thursday, 03/30/06, 9:00 - 10:30 a.m.*

MS Excel Basics  
*Wednesday, 03/22/06, 9:00 - 11:00 a.m.*

*Wednesday, 04/19/06, 9:00 - 11:00 a.m.*

MS PowerPoint  
*Friday, 03/24/06, 9:00 - 11:00 a.m.*

*Friday, 04/21/06, 9:00 - 11:00 a.m.*

MS Publisher Essentials  
*Tuesday, 04/11/06, 10:00 - noon*

MS Word Essentials  
*Wednesday, 03/29/06, 9:00 a.m. - noon*

MS Word Mail Merge  
*Friday, 03/31/06, 10:00 - noon*

Novell GroupWise Calendars & Proxy Rights  
*Thursday, 04/13/06, 10:00 - 11:30 a.m.*

Adobe - Creating PDF’s and PDF Forms  
*Wednesday, 03/29/06, 2:00 - 4:00 p.m.*

Short Courses are taught in Kettler Hall 205-B
Register at: [http://www.its.ipfw.edu/training/](http://www.its.ipfw.edu/training/)

---

**Microsoft Office 2003 Court Judgment and IPFW Response**

As many of you may be aware, it was recently decided in a court of law that certain portions of code found in Microsoft Office Professional Edition 2003, Microsoft Office Access 2003, Microsoft Office XP Professional and Microsoft Access 2002 infringe on a third party patent. Microsoft said it was forced to change the way its Access database interacts with its Excel spreadsheet.

According to the court’s decision, only new installations of these products must contain the new code. Current installations are grandfathered in.

Systems Administration reports that the MS Office 2003 and Office XP installation under IPFW Icons/Office Suites/Installs, has this revised code. We do recommend that you install MS Office 2003 rather than Office XP. We will be discussing the removal of the XP installation at some future date.

Any current installation of MS Office 2003 or XP is grandfathered in. However, any faculty or staff running MS Office 2003 who want the revised code can go to IPFW Icons > MS Office > Updates and run MS Office SP2.

Again, for MS Office XP users, we recommend upgrading to MS Office 2003; however, the revised code is also available under IPFW Icons > MS Office > Updates > Microsoft Office XP SP3.