

Data Integrity

Keep the Parishsoft Synchronizer Running (a.k.a. “The Pink People)

- Keeps the data you enter synchronized with the “mother ship” (AIM Server)
- Sync’s new data on the AIM database (i.e. info from other parishes) to your database. (btw AIM stands for Archdiocesan Information Management)
- Keeps the database backed up as it also runs the scheduled backup to the AoA ftp server.
- Check sync status regularly – Just because the pink people are in the system tray does not guarantee it’s doing anything.

Run Database Maintenance Regularly

- Database maintenance check
- Compact & repair
- How often is “Regularly”?
 - Depends on the amount of activity...
 - Large database/lots of activity – Weekly
 - Small database/little activity – Bi-weekly or monthly

Back Up Your Data Early and Often

- WHY BACK UP....?
- Disaster Recovery:
 - Fire, Flood, Theft, Disk Crash, Data Corruption....
- Parishsoft backs up to C:\Program Files\Parishsoft\Backup*day of week* in addition to copying to the AoA ftp server for off-site data
- Any other data that you consider "Important" should be backed up to removable media or at least another computer/server

Keep User ID's Current

- Add new user ID & password for new users
- Delete or inactivate old / unused user ID's
- Do NOT set up generic or shared user ID's
 - No accountability
 - Shared user ID's mean shared passwords; anyone can access/change data

File Sharing/Security on Server

- Put related data into its own share (Parishsoft, LOGOS, etc.)
- Create appropriate security groups for the shares
- Restrict access to only members of that group

Viruses

- Make sure you are running anti-virus software
- Keep it updated – Usually automatic but verify
 - Current virus signatures
 - Current anti-virus engine
- Make sure it is active/running
 - Verify antivirus icon is in the system tray
 - Test it with the EICAR test virus – Available from EICAR.ORG

Spyware / Adware / Malware

- What is it?
 - Monitors your surfing habits
 - Feeds ads / popups to your PC
 - Grabs user ID's, passwords, other personal information & sends it to its creator
- How does it get on my PC?
 - Drive-by installation
 - Tags along with "Cool Free Stuff"
 - Opening and/or clicking on links in infected messages

Adware / Spyware / Malware (continued)

- How do I know my PC is infected with Spyware
 - PC is suddenly slow/sluggish
 - Increased pop-ups / advertisements
 - New search or toolbar(s) in your web browser
 - Home page has been changed

Adware / Spyware / Malware (continued)

- How do I get rid of it?
 - Check Add/Remove Programs for “suspicious” programs (Link Optimizer, A Better Internet, Bargain Buddy...)
 - Anti-virus scan may catch some infections but dedicated Adware removal programs are specialized
 - AdAware (www.lavasoftusa.com)
 - Spybot S&D (www.safer-networking.org)
 - Store-bought programs (Spyware Doctor, AVG Anti-Spyware, Webroot SpySweeper...)

Last but not least: Windows Updates

- Keep your PC up-to-date with security updates & patches
 - Configure Windows Update to automatically download & apply updates
 - Or...
 - Manually update: Start, Programs, Windows Update
- Apply High Priority updates
 - Software & Hardware updates are optional. (if it works...don't fix it)
