Catholic Mutual. . ."CARES"

CYBER SECURITY TIPS

Parishes, schools and other Catholic organizations may be daunted by the perceived resources it takes to secure their computer systems; however, not making cyber security a priority could be a costly decision. The National Cyber Security Alliance recommends implementing the following key security principles to provide a starting point for a comprehensive security plan.

1. **Ensure that all employees use effective passwords.** Encourage passwords that are comprised of different characters and change them every 60 to 70 days, but no longer than 90 days. Passwords should be required to include both numbers and letters.

2. **Protect your systems.** Install and use anti-virus, anti-spyware and anti-adware programs on all computers. Ensure that your computers are protected by a firewall. A firewall can be a separate appliance, built into wireless systems, or a software firewall that comes with many commercial security suites.

3. **Keep all software up-to-date.** Ensure that all computer software is up-to-date and contains the most recent patches (i.e. operations system, anti-virus, anti-spyware, anti-adware, firewall and office automation software). Most security and operating systems contain automatic updates; make sure that function is turned on and sign up for security notifications from the software company. Without these updates, your systems will not be well protected against new cyber threats.

4. **Create backups.** Make regular (daily or weekly) back-up copies of all of your important data/information. Store a secured copy away from your office location and use encryption to protect any sensitive information about your institution and parishioners.

5. **Be prepared for emergencies.** Create a contingency plan so you can recover if you experience an emergency. Include plans to continue business operations at an alternate location when necessary. Test your plan annually. Make sure to erase all data on the hard drive before recycling or throwing away a computer.

6. **Report Internet Crime.** Locate and join an organization for information sharing purposes. If you suspect fraud or criminal intent, report it to local law enforcement agencies, the Federal Bureau of Investigation, Secret Service or the State Attorney General's Office.