CYBER THEFT—ARE YOU AT RISK?

Wikipedia describes cyber theft as “criminal activity where a computer or network is the source, tool, target, or place of a crime.” This activity and other computer crimes continue to be on the increase. Some examples of other computer crimes include fraud and identity theft; cyber stalking, phishing scams; information warfare; malware and malicious code; and denial-of-services attacks. Anyone can become a victim to these crimes if proper security precautions are not taken.

Recently, a Member location experienced a claim involving the theft of church funds using the church’s passwords and accounts. The thieves accessed the church’s computers through the internet and then transferred the money directly from the bank through a number of accounts in different countries to launder the money. It was reported that access to the church computers was gained due to current firewall and security patch upgrades not being updated. It is crucial that every location maintain their internet security by updating existing programs frequently. Older computers and outdated security make easy targets for these highly technical thieves.

The FBI reports another common theft opportunity occurs when a staff member is using church passwords. The home computer can be infected with a virus, unknown to the staff member, and the hacker is then able to access the church’s information on the home computer via the virus. Catholic Mutual recommends not allowing any church financial operations to be conducted on home computers to reduce the potential exposure to your church’s finances. If you do not currently have a procedure set with your bank, request that no wire transfers be conducted until a procedure has been established.

Alliance recommends implementing the following key security principles as a starting point for a comprehensive plan:

1. **Password** - Ensure that all employees use effective passwords. Encourage passwords that are comprised of different characters (i.e., numbers, symbols, upper and lower case) 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** - Install and use anti-virus, anti-spyware and anti-adware programs on 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 the computer software is up-to-date and contains the most recent patches. Most security and operating systems contain automatic updates; make sure that security and operating system updates are kept up-to-date. It is crucial that every location maintain their internet security by updating existing programs frequently. Older computers and outdated software make easy targets for these highly technical thieves.

3. **Update** - 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 the function is turned on and sign up for security notifications from the software company.

4. **Back-up** - Make regular (daily or weekly) back-ups of all 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** - 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.

6. **Report Crime** - If you suspect fraud or criminal intent, report it to local law enforcement immediately. Contact the Federal Bureau of Investigation, Secret Service or the State Attorney General’s Office.

7. **Stay Informed** - Do not open unsolicited attachments or email attachments. Internet fraud can be avoided by being cautious and scrutinizing the contents of messages that come through your computer. Parish churches 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.

Visit us on the web at www.catholicmutual.org

Catholic Mutual Group

Non-Profit Org.
U.S. POSTAGE
PAID
Permit #843
Omaha, NE

Catholic Mutual
Connection

Inside this issue

Shoes for Crews
Static at the Pump
WELCOME!
HINI
AED Success

Claims Story

Sara was stressed. As a volunteer for the youth ministry program at her parish, she had more to do for the Fall Youth Retreat than she could manage! When signing the final paperwork at the retreat center, Sara breathed a sigh of relief. This was one of the last issues on her list to take care of. She skimmed the contract, but so much didn’t make sense; what was “indemnify” anyway? Sara signed the contract and moved on to the next item on her list.

A few months down the road, Sara’s parish was named in a lawsuit to provide coverage for the retreat center. There were old pipes at the center and one had burst during the Fall Youth Retreat, causing a lot of damage. The retreat center had a contract stating that the church would be responsible for “any and all claims, whether due to the negligence of the church or retreat center while the church is renting the facilities.”

Unfortunately, this is an all too common occurrence. Catholic Mutual could argue that the church was not responsible, and possibly obtain a favorable judgment, but the costs to do so would be high. If Sara had understood what the contract meant, she would not have signed.

Catholic Mutual considers contract review an important part of our mission to protect the Catholic Church. Contract review is done to ensure that the contract is worded fairly, and the coverage required by the contract is available. In the aforementioned example, the contract Sara signed was fundamentally unfair because the retreat center should have required that the church assume responsibility for something that was a result of the retreat center’s own negligence.

Catholic Mutual has had much success in winning claims based upon unclear language in contracts. Our Risk Management Department has also developed an Addendum to Contract which, when signed by both parties, fairly allocates responsibility to each for their own negligence, and will amend the contract which was previously signed.

Catholic Mutual prefers to review your contracts or lease agreements prior to the contract being signed. We want to ensure that the insurance requirements in the document are in line with your coverage as well as provide you with guidance and direction when ambiguous language is included in the contract. In addition, you should make sure to have your Bishop or Director of Risk Management review the contract before you sign.

**Indemnify** means to compensate for damage or injury suffered.
According to the Center for Disease Control (CDC), H1N1 or swine flu, is a new influenza virus that was first detected in the U.S. in April 2009. By the end of July 2009, the CDC was reporting 43,771 total cases, which included 5,001 hospitalizations, and 302 deaths. On June 11, 2009, the World Health Organization (WHO) signaled that a pandemic of 2009 H1N1 flu was underway.

How does H1N1 spread?
The spread of the H1N1 virus is thought to occur in the same way seasonal flu spreads, mainly through coughing or sneezing by people with the virus. Touching something or somebody with the virus, and then touching your mouth or nose is another way this virus spreads. On the average, people with the virus can infect others from 1 day before getting sick to 5 to 7 days after for some younger or “at risk” individuals.

Your steps for prevention
• Get vaccinated when the vaccine is available.
• Wash your hands often with soap and water. Avoid touching your mouth, nose, or eyes.
• Cover your mouth and nose with a tissue when you cough or sneeze.
• Avoid contact with those that are sick.

What are the symptoms of H1N1?
The symptoms of this virus include fever, cough, sore throat, runny or stuffy nose, body aches, headaches, chills and fatigue. A significant number of people who have been affected also report vomiting and diarrhea, with severe illness and even death occurring as a result of this illness.

Who’s most at risk?
Although illness from H1N1 has ranged from mild to severe for all ages, those at higher risk for severe cases are 65 or older, children younger than 5, pregnant women, and people of any age with certain chronic medical conditions such as, but not limited to, diabetes, heart disease, asthma, and kidney disease.

Preparation steps for prevention
• Educate your employees on how the H1N1 virus can spread, and the symptoms to look for.
• Encourage employees and volunteers to frequently wash their hands or use alcohol based hand wipes, and make these items readily available.
• If symptoms exist, encourage employees and volunteers to stay home at least 24 hrs. after their fever is gone.
• Encourage employees and volunteers to get vaccinated when it’s available.

Four Easy Steps to Have Your Church Prepared for H1N1

1. Prepare a safety plan.
• Create a safety plan in conjunction with your local health department.
• Include an infectious disease response plan.

2. Establish a chain of command.
• Designate a crisis manager and a crisis team.
• Establish a recovery plan.

3. Hold a practice drill for your H1N1 response plan.

4. Contact Catholic Mutual and take advantage of our H1N1 programs.
• Get the new H1N1 discount by contacting Catholic Mutual.
• Check for other special coverage options.

www.catholicmutual.org

Connection
Vol. 8 No. 2. Fall/Winter 2009

Catholic Mutual
Catholic Mutual
The Roman Catholic Diocese of Albany,
The Roman Catholic Diocese of Dallas, and the Archdiocese of Vancouver, British Columbia

Catholic Mutual would like to take this opportunity to welcome several new members to our family! Please welcome -

The Roman Catholic Diocese of Albany,
The Roman Catholic Diocese of Dallas, and the Archdiocese of Vancouver, British Columbia

According to the Center for Disease Control (CDC), H1N1 or swine flu, is a new influenza virus that was first detected in the U.S. in April 2009. By the end of July 2009, the CDC was reporting 43,771 total cases, which included 5,001 hospitalizations, and 302 deaths. On June 11, 2009, the World Health Organization (WHO) signaled that a pandemic of 2009 H1N1 flu was underway.

How does H1N1 spread?
The spread of the H1N1 virus is thought to occur in the same way seasonal flu spreads, mainly through coughing or sneezing by people with the virus. Touching something or somebody with the virus, and then touching your mouth or nose is another way this virus spreads. On the average, people with the virus can infect others from 1 day before getting sick to 5 to 7 days after for some younger or “at risk” individuals.

Your steps for prevention
• Get vaccinated when the vaccine is available (scheduled for this fall).
• Cover your mouth and nose with a tissue when you cough or sneeze.
• Throw tissue away after use.
• Wash your hands often with soap and water.
• Avoid touching your eyes, nose, or mouth, when possible.
• Avoid contact with those that are sick.

What are the symptoms of H1N1?
The symptoms of this virus include fever, cough, sore throat, runny or stuffy nose, body aches, headaches, chills and fatigue. A significant number of people who have been affected also report vomiting and diarrhea, with severe illness and even death occurring as a result of this illness.

Who’s most at risk?
Although illness from H1N1 has ranged from mild to severe for all ages, those at higher risk for severe cases are 65 or older, children younger than 5, pregnant women, and people of any age with certain chronic medical conditions such as, but not limited to, diabetes, heart disease, asthma, and kidney disease.

Preparation steps for prevention
• Educate your employees on how the H1N1 virus can spread, and the symptoms to look for.
• Encourage employees and volunteers to frequently wash their hands or use alcohol based hand wipes, and make these items readily available.
• If symptoms exist, encourage employees and volunteers to stay home at least 24 hrs. after their fever is gone.
• Encourage employees and volunteers to get vaccinated when it’s available.

Four Easy Steps to Have Your Church Prepared for H1N1

1. Prepare a safety plan.
• Create a safety plan in conjunction with your local health department.
• Include an infectious disease response plan.

2. Establish a chain of command.
• Designate a crisis manager and a crisis team.
• Establish a recovery plan.

3. Hold a practice drill for your H1N1 response plan.

4. Contact Catholic Mutual and take advantage of our H1N1 programs.
• Get the new H1N1 discount by contacting Catholic Mutual.
• Check for other special coverage options.

www.catholicmutual.org