Catholic Mutual. . .CARES

PROTECTING YOUR NETWORK FROM INTERNET/EMAIL RISKS

Loss of valuable, confidential data, downtime and damaged systems are not pleasant issues to deal with. They can cost your organization a significant amount of money, not to mention the time involved to resolve the problems. Properly securing your computer from the numerous threats posed by viruses, spyware and hackers is just as important as being aware of the Internet's dangers. A brief investment of time and effort is all that it takes to make sure that your computer remains free of malicious software and is off limits to hackers. Implementation of the following measures will go a long way to protect your local area network (LAN). All organizations should have an IT individual or staff that would be responsible for overseeing these safety measures:

- Limit floppy drive access, USB ports and serial ports on networked computers. These are the most common entry points for problems and most users do not need access to these drives. They can email or store data elsewhere in a safe "scanned" environment.
- Do not allow any users to modify any system files. All network users should be locked down so they can only perform tasks which administration has agreed upon.
- Block Instant Messenger. These send messages and attachments out to a server and then back to its clients. By disabling its functionality, viruses and other computer risks can be controlled from spreading.
- A current subscription of antivirus software should be run on all your computers. Some examples include Norton Antivirus and McAfee Virus Scan.
- Install a firewall which helps prevent unauthorized sources from entering or leaving your computer, making you invisible on the Internet. A firewall should always be used if you have a broadband connection (DSL or cable). Some examples include Zone Alarm Pro 2007 & private firewall.
- Install anti-spyware software on each computer. Spyware software monitors or controls your computer use and is used to send you pop-up ads, redirect your computer websites, monitor your Internet surfing, or record your keystrokes. Some examples include Spybot Search & Destroy or Spyware Doctor.
- Never open attachments to an email unless you trust the sender as this is often what triggers a virus to enter your computer.

- Install filters to prevent users from accessing forbidden sites. Consider using a mechanism which allows you to monitor or track an individual users' behavior on the web.
- Install a port monitor to prevent your ports from being scanned. Hackers regularly try to find and exploit weaknesses in operating systems and web browsers.
- Require passwords to be changed frequently and the password must not be the same as any of the previous six passwords. Passwords should contain both letters and numbers or symbols.
- Require the combination of key strokes CTRL+ALT+DEL to logon. This provides an additional security layer requiring the user to physically be at the computer to log on.
- Use password-activated screen savers to lock computers after a period of inactivity.
- Continuously update your operating system and web browsers. Most can be set to check for updates automatically.
- Maintain backups of your software applications and files at a secured, off-site facility. Use encryption to protect any sensitive information.
- Enact an Email and Internet Policy. All users should be given a hard copy to read and required to sign and date they have read and understand the policy.
- Develop and implement a Security Plan and train users properly to ensure confidential information is kept secure.
- Avoid putting photos of individuals on your website, especially minors, unless photos are located under an area that is password protected.
- Ensure your IT individuals are up-to-date on the latest technology.

(Revised 02/2021)