CYBER SECURITY PRACTICES

STAYING SAFE ONLINE

The widespread availability of computers and connections to the Internet provides 24 hour access to information, credit and financial services, and shopping. The Internet is also a great communication and learning tool for educators and students. People have begun in expect instant access to information from a wide variety of sources, including the Catholic Church. The Church is being asked to provide online services creating the concern for safeguarding sensitive data. A breach in the church's information security system could result in an unintentional disbursement of confidential information including parishioner's personal information, or financial or personnel records for the church.

Unfortunately, there are people who take advantage of the Internet through criminal behavior and other harmful acts. These criminals try to gain unauthorized access to your computer and use that access to steal identities, commit fraud, or even launch cyber attacks against others.

The National Cyber Security Alliance recommends adhering to the following cyber security practices. These practical steps will help your parish/school and staff stay safe online to avoid becoming victims of fraud, identity theft, or cyber crime.

❶ Protect Personal Information

Criminals are very interested in obtaining personal information. The reality is that anyone can be a victim of identity theft. According to a recent Federal Trade Commission survey, almost 10 million people are the victims of identity theft every year. The following steps should be followed while online to minimize your risk of identity theft:

- Before giving out personal information (i.e. name, address, account numbers, social security number), learn how it will be used and how it will be protected.
- Do not open unsolicited emails or those from unknown sources.
- If making a purchase online, do not provide personal or financial information unless you have checked to ensure a site is secure. Examples include a "lock" icon on the browser's status bar or a website URL beginning with "https:".
- Read and understand a website's privacy policy. This details what personal information is collected by the site, how the information is used, and if information is passed along to third parties.

❷ Know who you're dealing with

- **Phishing** – "Phishers" send spam or pop-up messages claiming to be from a business or organization that you might deal with on a regular basis (i.e. your financial institution, an Internet Service Provider (ISP), a governmental agency). This is the "phishers" way of tricking you into divulging personal information so they can steal your identity. Never open unsolicited email messages; don't open attachments from people you don't know or don't expect; and don't reply to or click on links in email or pop-ups that ask for personal information via email. Legitimate companies never ask for this information in this manner. Verify the request by calling the company directly; however, use a contact number on a recent statement instead of one given on the email.

- **Free Software and File Sharing –** File sharing entails downloading special software that connects your computer to a network of other computers running the same software. By not checking the proper settings, you run the risk of allowing access to other information on your hard drive, instead of just the files you originally intended to share. Downloading file-sharing software is not advised and could place personal information and your computer at risk.

- **Spyware** – Spyware is software installed without your knowledge or consent that adversely affects your ability to use your computer, sometimes by monitoring or controlling how you use it. In some cases, it can also use your computer to access or launch attacks against others. All computers should have some type of anti-spyware software installed to scan for and delete any spyware programs that may sneak onto your computer.

- **Email Attachments and Links** – A virus sent over email cannot damage your computer without your help. Never open an email attachment unless it's from a known source or you know what it contains. When sending emails, help others trust your attachments by including a message in your text explaining what you are attaching.

❸ Use anti-virus software, a firewall, and anti-spyware software

- **Anti-virus Software –** Anti-virus software protects your computer from viruses that can destroy your data, slow your computer's performance, cause a crash, or even allow spammers to send email through your account. It works by scanning your computer and your incoming email for viruses and then deleting them. Anti-virus software must be updated routinely. Most commercial anti-virus software includes a feature to automatically download updates when you are on the Internet. When deciding on a brand of software, keep in mind that good anti-virus software should recognize current viruses, as well as older ones; effectively reverse the damage; and update automatically.

- **Firewalls** – Firewalls assist to keep hackers from using your computer to send out your personal information without your permission. Basically, it acts as a guard watching for outside attempts to access your system and blocking communications from and to sources you don't permit. Many operating systems and hardware devices come with a built-in firewall. To ensure your firewall is effective, ensure it is turned on, properly set up and updated regularly.

- **Anti-Spyware Software** – Anti-spyware software helps protect your computer from malicious spyware that monitors your online activities and collects personal information while you surf the web. Since the sophistication of spyware programs is increasing, consider using two different anti-spyware programs to offer increased protection.

❹ Proper set up of operating system and Web browser software

- Hackers take advantage of unsecured Web browsers (i.e. Internet Explorer) and operating system software (i.e. Windows). Lessen your risk by changing the settings in your browser or operating system and increase your online security. Built-in security features can be found in the "Tools" or "Options" menus.

- Your operating system may offer free software patches that close holes in the system that hackers could exploit. In fact, some common operating systems can be set to automatically retrieve and install patches for you. If not, make regular visits to your system's manufacturer website and update your system with defenses against the latest attacks. Your email software may assist in avoiding viruses by providing the ability to filter certain types of spam; however, you must activate the filter.

❺ Passwords

- **Protect** your passwords by keeping them in a secure place and out of plain view. Never share your passwords on the Internet, by email, or by phone.

- **Strengthen** your password by making it harder for hackers to figure them out.

    - **Use passwords that have at least eight characters and include numbers and symbols.**

    - **Avoid common words**

    - **Never use your personal information or login name as password**

    - **Change your passwords regularly (at least every 90 days)**

    - **Use a different password for each online account you access**

❻ Back up files

- No system is completely secure so it's important to copy important files onto a removable disc and store securely in a building other than where your computer is located. If a different location is not practical, consider encryption software. This software scrambles a message or a file in a way that can be reversed only with a specific password.
- Always keep your original software start-up disks handy and accessible for use in the event of a system crash.

❼ Learn what to do if something goes wrong

- **Hacking or Computer Virus** – If your computer gets hacked or infected by a virus:
    - Immediately unplug the phone or cable line from your machine. Then scan your entire computer with fully updated anti-virus software and update your firewall.
    - Alert the proper authorities by contacting your ISP and the hacker's ISP (if you can tell what it is). Often, the ISP's email address is abuse@yourispname.com or postmaster@yourispname.com. Include information on the incident from your firewall's log file. Also, alert the FBI at www.ifccfbi.gov.
- **Internet Fraud –** All fraud related complaints should be reported to the Federal Trade Commission (FTC) at www.ftc.gov. They enter Internet, identity theft, and other fraud related complaints into Consumer Sentinel, a secure, online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.
- **Deceptive Spam** – If you receive deceptive spam, including email phishing for your information, forward it to spam@uce.gov. Be sure to include the full Internet header of the email. For further information, go to http://getnetwise.org/action/header.
- **Divulged Personal Information** – If you believe you have mistakenly given your information to a fraudster, file a complaint at www.ftc.gov and then visit the Federal Trade Commission's Identity Theft website at www.consumer.gov/idtheft to learn how to minimize your risk of damage from a potential theft of your identity.

*****Information provided by the National Cyber Security Alliance*****