

# Safe & Sensible Computing

By: Carole Oat



**KEEPING YOUR COMPUTERS RUNNING WELL AND FREE** from viruses and malware is a must for every company. Following the best practices outlined below will go a long way in keeping club data and the private data of club members safe, along with ensuring that your computers run at maximum efficiency 24/7, 365 days a year. The old adage, “an ounce of prevention is worth a pound of cure,” has never been so true.

## UPDATE YOUR OPERATING SYSTEM REGULARLY

Installing Windows updates is highly recommended. On the second Tuesday of each month, Microsoft releases important security patches, updates, and enhancements; emergency patches are released as soon as they are available. If your system is not up to date, it is vulnerable to a host of possible security threats.

## KEEP YOUR ANTIVIRUS SOFTWARE UP TO DATE

Get antivirus software installed on every computer in your club. If you do not have this protection, you are vulnerable to malicious attacks from a number of sources. Remember, antivirus software is only effective if it is up to date. Most, if not all, antivirus software will automatically update itself, however it should be checked manually as well.

## REMOVE INAPPROPRIATE SOFTWARE FROM COMPUTERS

Periodically, take an inventory of the software installed on your computers and determine if it is necessary to run the business. Since it's easy to download and install programs from the Internet, you may find programs that are really not necessary. While some programs are benign, many others come bundled with embedded malicious software. You should remove any unnecessary software; the benefits will be better security and production from your employees. If there's a program you are unsure of or unfamiliar with, research it before you uninstall it.

## KEEP YOUR CLUB MANAGEMENT SOFTWARE UP TO DATE

Most software companies continually release updates. Ask your provider for a list of these, and how you can change your settings

to get them automatically as they are released. Software companies respond to ongoing threats – applying updates can not only allow you to take advantage of security advances, but also allows you to use features and functions that are frequently added.

## WORK WITH A PCI-DSS COMPLIANT SOFTWARE AND BILLING COMPANY

What's more important to your business than the trust relationship you have with your members? The financial information they have placed in your care must be secure, for their protection as well as yours. A single breach of this trust – even if no real harm was done – could irreparably damage a club's reputation.

To provide you and your members with the highest possible level of cardholder data security, work with a software and billing company that is fully PCI-DSS Compliant. PCI-DSS (Payment Card Industry - Data Security Standard), originated in 2004 when the CISP (Cardholder Information Security Program) requirements were incorporated and updated into this new standard. PCI-DSS was developed by the PCI Security Standards Council – a consortium of major payment card brands – to enable companies of all sizes to employ consistent data security measures.

## DEVELOP A PLAN

Starting with the points above, every club should create a data security plan. Work with your software provider to create a schedule of events to keep your club safe:

- **MAINTAIN** an information security policy that includes protocols for email and Internet use by employees – strict password management and the assignment of a unique ID to each person with computer access.
- **INSTALL** and maintain a firewall.
- **MONITOR** and test access to network resources, cardholder data, security systems and processes.
- **INSTALL** battery backups on all computers.
- **ENCRYPT** transmission of cardholder data.
- **RESTRICT** access to data on a need-to-know basis.
- **RESTRICT** physical access to cardholder data.
- **USE** a disk clean-up utility and defragmenting software to help your computers run more efficiently.
- **MAKE** frequent back-ups of your data and store that information off-site.
- **LIMIT** use of email from your domain to prevent being labeled a spammer and getting blacklisted.
- **MINIMIZE** the number of administrator log-ins to prevent users from downloading inappropriate software.

CAROLE OAT IS THE NATIONAL SALES MANAGER FOR TWIN OAKS SOFTWARE. SHE CAN BE CONTACTED AT 866-278-6750, OR BY E-MAIL AT COAT@TOSD.COM. VISIT US ON THE WEB AT WWW.TOSD.COM.