Small Business News & Notes

Keeping Hard Drives Healthy

(NAPSA)—Many small business owners now provide health care not only to their employees, but to their computers as well. Virus protection software has become commonplace in the small business world. While much of the software is effective, however, experts caution it is not perfect.

Try these tips from data security company Norman Data Defense Systems to back up your virus protection systems—for free.

Step One: Stop viruses from entering through the A drive. Floppy disks often contain viruses that enter a computer during boot up. Change your boot up sequence from “A then C” to either “C then A” or “C Only.”

Step Two: Stop viruses that need the Windows Scripting Host (a facility within Windows that executes Visual Basic and Java Scripts) to infect. Go into “Control Panel” and then “Add/Remove Programs.” Select the “Accessories” button from the “Windows Setup” tab. Deselect the Windows Scripting Host option.

Step Three: Prevent harmful content from running when a Word document is open. Download and install the Office Viewers for Word, Excel and PowerPoint (free at www.office.microsoft.com/Downloads/default.aspx).

Select your product and check the box that says “converters and viewers.” Hit “update list.” During installation you will be asked if you want to use that particular office viewer as the default viewer for Word documents. By choosing “Yes,” every time you double click on a Word document, you will view the document only and prevent harmful content from running.

It’s important for small business owners to protect their computers from viruses.

Step Four: Disable options in Browser software that may run harmful code. Options in browser software often let viruses enter a system. Because most people don’t use these options, it’s best to cut them off to keep viruses out. With Internet Explorer, options can be accessed by going to Start Menu>Settings>Control Panel>Internet Options>Security. Set the slide bar for the highest security possible.

Step Five: Stop viruses that hide in e-mail attachments. When you get an e-mail with an attachment, think before opening it. Does the e-mail have a strange title? Does the attachment have an odd name or a strange extension? Is it from a person you exchange e-mails with often? If in doubt, delete the entire e-mail. Discourage your colleagues and associates from sending attachments and stop sending them yourself. It is often just as easy to send information as URLs, rather than attachments. This format does not carry viruses, has no size and can be referred to as often as needed.

For more information visit www.norman.com/us.