Virus Protection Procedures

We want to warn our clients and friends of some of some security issues which may be even more important to understand in the coming days, and have put them in the following list:

1. Do: back-up all important files on your computer(s) and keep a copy in a location other than the computer location, preferably a safe deposit box.
2. Never, never, never open attachments to emails from an unknown source. Delete the email immediately.
3. Even with E-mail from someone you KNOW, DO NOT open attachments unless and until you have separate information from that source as to the type of attachment and it's contents. Even then, do not open it unless you have up-to-date anti-virus software properly installed on your computer. Doing so could lead to loss of data.
4. Certain spread sheets and other program or executable files attached to E-mails can contain viruses of which the sender is NOT aware. So take no comfort if your friend tells you an attachment did not damage their computer; Virus actions are frequently RANDOM.
5. If you visit Web Sites linked in an unsolicited email message, those Web Sites frequently collect personal information from your computer which, at best may cause you to be placed on more junk email lists, and at worst can steal credit card and other personal information stored on your computer. Many such programs ONLY require that you click a button, usually marked "ENTER" to start this clandestine information collection process.
6. If you have responded to random "Chain" emails in the past, whether for prayers or for the hope of winning money or

vacations, please STOP. Terrorists and their supporters can easily use such tools to create millions of false trails for authorities to follow, thus thwarting efforts to locate and bring them to justice. Likewise, remove any unknown or outdated E-mail addresses from your E-mail address book.

7. Don't: ever respond to an E-mail that offers to "remove you from an E-mail list". They are usually simply verifying your E-mail address so they can sell it to others for more money.
8. Do: install anti-virus software and update it every two weeks, or at minimum, once each month.
9. Use only software updates available from legitimate Vendor Website downloads such as Windows Update. Never download software offered in an unsolicited email, unless you know it is from a legitimate source.
10. If you are not sure if your computer is running up-to-date anti-virus software, you may want to visit the following Web Site to run free security checks available from Symantec, publisher of Norton AntiVirus software: http://security1.norton.com/us