



Customer Focus on Loss Control

Innovative Safety and Health SolutionsSM

Guarding Against E-Mail Viruses

E-mail virus attacks have been a serious and consistent concern for businesses of all types and size. Recent attacks by e-mail viruses have damaged computers, corrupted business data, and caused the loss of critical access. According to Computer Economics, the global cost of business interruption, lost productivity and cleanup costs in 2001 were estimated at \$17 billion dollars. The National Computer Emergency Response Team (CERT) estimates that the number of attacks rose from 21,765 in 2000 to 52,658 in 2001. Why all this focus on e-mail? After continued attacks, businesses learned to harden security on their networks with firewalls and other intrusion detection software. But many businesses have not equally protected e-mail servers. These less-protected access points allow hackers to bypass network security measures. Less vigilance and less protection on the part of businesses, coupled with the unwitting assistance of many unwary or uninformed e-mail users, give virus creators an ideal way to propagate their malicious payloads. Every individual and business should follow these security tips:

- Make sure that you install a recent version of anti-virus software on every computer on your network and every computer that connects to your network. Insist that all friends, associates, business partners, vendors, and suppliers use updated anti-virus software.
- Because new viruses appear almost daily, be sure that your company has plans to regularly update all copies of anti-virus software with the newest "virus signature" or "virus definition files" at least weekly. These update files allow your older anti-virus programs to detect newer viruses and their variations earlier and more successfully. With most software, these virus updates are available for free for the first year.
- For best results, set up anti-virus software to scan automatically every time you start your computer, and to run continuously in the background during any on-line activities and anytime you receive, open, or modify files. Those who rely on manual scanning often forget to run scans frequently enough to offer the fullest protection.
- Consider deleting, unopened, unexpected or unrequested e-mail, or email from someone you do not know.
- E-mails that look suspicious probably are. Consider deleting, unopened, any message with a blank subject line, a subject line with numbers, random letters, or other unusual greeting. Overcome the "curiosity factor." Any legitimate person trying to contact will try again or use another method.
- If you get a suspicious looking e-mail from a person you know, it may be that that person's machine is infected and is sending a virus to that person's entire e-mail address book. Contact that person by telephone or other means to ask about the suspicious e-mail. Your contact may not even be aware that his or her PC is infected.
- When you open an e-mail message, even one from a known or trusted source, do not automatically open any attachments. Viruses are most commonly sent in "trick" attachments that launch the virus when the file is opened. Do not open any attachments that have the following types of extensions at: .exe, .com, .sys, .dll, .vbx, .ovl, .bin, .drv. Each of these file types can deliver a virus. Look out for especially tricky file names such as *monthly budget.exe* or *vacation pictures.vbx* or *attachment.com*. Never double click on such files.
- Consider scanning every e-mail attachment, even one from a known or trusted source, before you open it. Even if a file is a legitimate, expected attachment from a trusted friend or associate, it could be infected.
- Consider installing a "scan mail" program just ahead of your e-mail server. It can act as a kind of firewall for your e-mail. These programs can scan every e-mail for suspicious attachments, and can "quarantine" e-mail that has special patterns or wording. (It can also be helpful in eliminating annoying junk e-mail.) Installing a scan mail program together with anti-virus software on every computer is a good starting point for protection against business interruption, computer damage, loss of data, lost productivity and the potential embarrassment of appearing on the front page of every newspaper identifying you as the latest unprepared victim.
- Create a policy for acceptable use of e-mail. Educate employees about the inherent risks of e-mail. Create e-mail and access guidelines for all employees, and share these during orientation and continuing education.

