



# Pennsylvania Lumbermens Mutual Insurance Company

Is there **TERRORISM** in **YOUR WORK PLACE?**

You'd better believe there is and it is not only in your work place but also in your home. Why do I say this? Well, if you own a computer then you are a prime subject for a terrorist attack.

In a recent meeting held in Greensboro, NC at the 72<sup>nd</sup> Annual NC Statewide Safety Conference, I listened to David Martinez, a Special Agent with the FBI, speak about terrorism and how it may impact all of us.

One of the things that he talked about was the use of computers in the work place. Most companies, whether a one-man operation or a large corporation, use computers and usually more than one person has access to the computer. The bottom line is that both domestic and foreign countries are having a rash of computer problems that come in the form of viruses. Computer hatcherers and those who create these viruses (domestic and foreign) are committing acts of terrorism.

Many times these viruses will start in another country and they spread or have a rolling effect as the sun rises in each of the various time zones and as workers sat down at their computers. Hopefully, by the time the virus has reached the U.S., we have received a warning to watch out for the virus and that our various virus protector programs will be able to quarantine the virus. I thought it was ironic that the week I was hearing this information the following happened: my home computer quarantined two virus problems, my wife's work place was hit with a virus and several warnings came from computer experts to not open email from anyone you did not know, or not to open any attachments to email from anyone.

Some of the things we can do to help control this outbreak of computer terrorism are:

- 1- **HAVE** a good virus detector program on your computer and **KEEP** it **UP-DATED** either daily or weekly.
- 2- **DON'T OPEN ANY EMAIL** from anyone you do not know. Remember; even if you know them it still may not keep you from getting a virus from someone you know. Many viruses automatically send to all addresses in your email address book.
- 3- **SCAN** your outgoing email with a virus protector to insure that you are not sending a virus through your email.
- 4- **DON'T** let **UNAUTHORIZED** personnel use your computer. Sometimes they may not be aware of the virus danger or they may create unwanted email for you.
- 5- **WATCH OUT** for those special offers you get in emails or programs that may have been copied or handed down from one person to another – they may contain a virus.
- 6- **BACKUP YOUR COMPUTER DATA** either daily or at the very minimum weekly.

One Commerce Square • 2005 Market Street, Suite 1200 • Philadelphia, PA 19103-7008

Main 800.752.1895 Fax 215.625.9097

[www.plmins.com](http://www.plmins.com)



PLM:: Service

7- KEEP at least one set of backup data somewhere other than at work to be on the safe side.

8- REMEMBER whether you want to admit it or not you are under attack and having your computer system wiped out can be VERY STRESSFUL.

All computers should have surge protectors, power storage backup devices, and power and phone lines coming into all electronic equipment should be grounded.

If you have a computer technical person or computer company you use for assistance, you may want to talk to them about making sure your system is as safe guarded as possible. In turn, they may be able to offer you some other suggestions to further protect your information and investment.