The Geeks Speak

“BioHazard!”

The Geeks Speak is a periodic electronic publication of Hargraves Computer Services offering helpful tips on various computer-related issues.

This issue's soapbox has a big "BIOHAZARD" sign stamped on its side. (Maybe it should be “DATAHAZARD”, but then you might not get the joke!) The Klez virus is still making the rounds. The newest threat is BugBear, which you may have seen on the news recently. We get a dozen or so notices a day from our mail server's antivirus scanner regarding Klez, and we've already gotten a few BugBears as well. Fortunately, Norton Antivirus for Exchange is peeling them out before they get to our users. This nifty product looks at everything before it gets to the users so nobody has to think about whether it's safe to open an attachment. (You can have this protection, too – just let me host your mail services, wink-wink!)

Those of you not on an Exchange server with this wonderful antivirus tool must be a bit more careful. The often-repeated line about never opening attachments you aren't expecting is still a good one, and one not adhered to enough. Keeping your virus definitions up to date is a must, and re-upping your subscription when it tells you to is imperative.

Regarding the BugBear worm: Although we haven't had to clean up a BugBear infection yet, according to Symantec the worm often doesn't show obvious symptoms of infection. It opens ports on the infected machine, monitors the keyboard to intercept passwords, and gives the information back to the hackers. You may not notice any of this, and probably the hackers have more inviting targets than you to attack. However, the possibility exists that you may be vulnerable to attack without any overt signs of infection. Up to date definitions and subscriptions will protect you, as long as they haven't been bypassed. But, if you're unsure whether you've been practicing safe computing you might want to update and scan just to be sure. A quick and dirty check is to look at the contents of your startup folder. BugBear places itself in the startup group in the format ???.exe, where ??? represents three characters chosen by the worm. If you have an item in this format sitting in your startup group, it's not necessarily the virus, but it sure bears investigating!

Regarding the Klez worm: I'm getting a lot of calls from clients who have virus protection in place, they aren't bypassing it, they keep their definitions and subscriptions up to date, perform periodic scans, blah blah blah. Then one day they get a nasty-gram from someone else's network informing them that they are infected by the Klez virus. Klez will forge the headers of the emails it sends out, making them appear to be from someone in the infected machine's address book, rather than from the user of the infected machine. An informed network administrator realizes this and accounts for it. But some networks are maintained by non-IT people who might not be aware of this aspect and may send messages out erroneously. I wouldn’t get too worked up over this, but of course anytime you’re accused of spreading a virus you need to look around and make sure your house is in order.

In summary, practice safe computing, especially safe email. Update your definitions and subscriptions, and of course, if you’re unsure about anything, please don’t hesitate to call.

That’s it for my soapbox speech of the week.
As always, thank you for your continued business!

Sincerely,

Terry Hargraves

Hargraves computer services

281.252.3603