Northern California Chapter
Electronics Representatives Association

NCALERA NEWS

SPECIAL REPORT on SOUTHERN CALIFORNIA CHAPTER MEETING – August 24, 2004

PRACTICE SAFE COMPUTING

By Bob Parsons

The publicity surrounding this ERASCAL Owner's meeting was dynamic to say the least. We were not disappointed by the amount of data that was sent our way. We may have gotten a little confused at times, but here goes!

The target topics covered a pretty broad, no, *busy* spectrum. Viruses; Spam; Hardware Failure; Theft of personal & business data; with a smattering of discussion about the ERA Website and Directories. Overkill? Well, read on.

The "experts" on the panel (shown below in the order shown) were well selected:

Dennis McGillis, ERASCAL Executive Director, who put this all together and hosted the program.

Bill Perry, Pertel Communications, ERASCAL's webmaster and key contact for NCALERA's computer gurus. Bill ties all the ERASCAL's technical activities together.

Andy Adams, Cox Cable (prominent in Orange County) is their communicator of bad news. When a customer has a bad response, virus infections, spam attacks, it is Andy's department that gets involved.

Gerry Teudt (pronounced (Toyt) is SBC's DSL expert in their area. His role is not that far from that of Andy, above, but in the copper-wire domain.

Jeremy Bowden, Cloud 80, a local ISP/Web Host for many of the reps present. It was he who answered many of the spam-related challenges that were addressed.

☼ OPENING COMMENTS

had pretty much to do with Virus infections of all types. Quite as expected, there were mentions galore about the SP-2 Service Pack released for Windows XP. The general recommendations of those present were to install the Service Pack right away, particularly for smaller, single-user and small network users. Yes, certain ISP's have made requests for certain modifications to be made. Mostly these effect some of the special functions such as parental controls and the like. Of importance, if an ISP suggests that you make changes and you notice challenges in operations, change it. If everything is working OK – leave it alone. Just remind yourself

that this is part of Microsoft's efforts to correct existing "holes" in their security apparatus in and around Windows, particularly XP.

Editor's Note: We have XP Home and have installed SP-2. So far, we have had a few challenges. Of those found, one method has been to uninstall and re-install the program. Another required a new driver, and then another uninstall and re-install.

The discussion was clouded slightly at this point, combining the need 1) to put anti-virus program up-dates into effect with 2) the need to stay up-dated with your Windows up-dates. Both can be set up automatically and it was recommended that one do so wherever possible. On the other hand, users are warned that the automatic up-dates are not attached to an iron-clad guarantee. Schedule yourself to up-date manually at least once a week – certainly once a month!

Finally, Gerry of SBC reminded us to make certain that your anti-virus definitions are current. Some programs, such as Norton System Works, automatically check this and notify you on their status window. If you use other anti-virus programs, check this out. This is one thing that may change on a daily basis. Do it at least weekly.

☼ **SPAM . . .**

was the topic that dominated the discussion during the first half hour and then spilled over heavily into lunch. During the introduction, people commented about getting thousands of e-mail messages in a given day. From what we read, that timing could have been in an hour – or less.

Why does spam exist? Well, it was pointed out during the presentations that surveys have determined that over 40% of the internet users actually open spam regularly and (get this) actually purchase products as a result. When one thinks of the literally millions of message-offers that are routinely sent out every day, it

is no wonder that spammers will do almost anything to continue their activities.

Keep in mind that spammers are not that far removed from virus writers. Both groups are highly motivated. Virus writers have some kind of psychological challenge, something that drives them to be insane devils. But the spammers are good guys just like the rest of us. What they do is done for *money!* Consider what kind of dollar returns they get as a result of those 40% who look at their offers. We read comments about the billions of dollars spent each year on pornography alone, for instance.

Just as viruses "worm" their way from computer to computer, spammers get through the defenses put up by firewalls and anti spam programs and take over the computer's functions, sending out their messages in large bursts, then going on to another computer station and repeating its illegal activities. In case of networks, once a station has been penetrated, the take-over process sets in to capture the entire network. Since they are behind the main firewall, there is little to impede their progress.

Your ISP can become a savior to your time and temperament, saving you from being attacked.

The ISP's are the ones who have to set up filtering devices that identify these large intrusions by any given customer. Your ISP can become a savior to your time and temperament, saving you from being attacked.

However, because ISPs do not read each message, they frequently tend to get in the way. They screen out good messages as well as bad, sometimes with terrible results. To help prevent this, they establish Black and White lists, lists which identify the good guys (white lists) and the bad (black lists).

We have faced another result of these well-meaning ISPs. We found it impossible to send out blind copies to our membership listings, for instance. Because we do not work through the chapter website, our *sending* address does not reflect NCALERA. Our *receiving* address does. Our members do not find it that difficult to deal with this difference since they don't have to be around very long before that address distinction becomes routine. (Yes, we do send out a lot of e-mail correspondence.)

Enter anti-spam programs. Several of our members install anti-spam programs on their set-ups and we get blacklisted if we use bulk mailing techniques. We have solved most of our problems by going to a mail-merge system where each message is individually addressed (Dear John or Jane) and individually sent. While it takes more time, it has paid off by having a greater assurance that each member will get our messages. We send out messages in the low hundreds. Think what a challenge this might become if we were in the thousands?

Well there are solutions, however fleeting. It came out during the meeting that one can communicate with their ISP and get a special listing established, another form of white list. One such action involves a process called, Reverse DNS. For the technically challenged among you, the internet does not send out all those names we are so accustomed to using. Something or somebody @NCALERA.ORG or @ERASCAL.ORG or the last half of your address. These Domain-name-related addresses are converted to IP addresses, a series of numbers such as 192.0.2.25. Your ISP can set it up so that your messages are identified and sent using the IP address. Your received mail is converted the other way.

Look up http://www.dnsstuff.com/info/revdns.htm "How Reverse DNS Works" for a complete technical discussion of this procedure. It is not difficult reading, but it does take two pages of copy to get it all down. Just know that all this effort is to identify you as being real or legitimate.

Bill Perry reminded us that even this latter process can be "broken" or "spoofed." There is no perfect solution to any of these things because the problems are so dynamic! As fast as you come up with a solution, they come up with another way around you. To paraphrase a great Patriot, "Eternal vigilance . . . "

Intermingled in these conversations and write-ups is the mention of "firewalls." We cannot tell you how casually the people who attended this meeting were using the term. This could be an indication that firewalls usually work well, or that the audience didn't have a clue as to how they worked . . . Or a little of both?

WE WATCHED AND LISTENED

LARRY AND MANA's
HELEN DEGLI-ANGELI

Suffice it to say, there are software and hardware versions. Hard is better and is usually included in a router or wireless access point. If you are having challenges around the process, look it up on your favorite search engine resource – Yahoo, Google, what-have-you.

There are some things you might want to do right away. You may have an e-mail address showing on your personal or company website that is designated and designed to operate as a "catch-all" address. A few years ago, this was considered a very worthwhile addition to your site. This kind of address, often shown as info@yoursite.com picked up all the misspelled addresses. R, Robert, Bob, boob (in my case) or any other typos were funneled into this catch-all box and you didn't miss messages improperly addressed. This plays right into the spammers hands, however and such addresses should be eliminated. Change the address shown on the website to Postmaster and call your ISP or webmaster to determine how to complete the change on your system.

And never, ever click on the spammer's instructions at the bottom of the message to delete your name from their mailing lists. That is an invitation to spammer's hell. Never!

BACKUPS

The heading is plural because there are so many ways to back up your data. Before we get into the ways, let's review the necessity. The opening statements around this topic had to do with the MTBF (Mean Time Before Failure) of hard drives. It was noted that some offer over 10 years of life.

Bill Perry commented that three to five years is a more realistic picture – that when that fifth year has passed, one should not be surprised by hard drive problems. He cited ways of observing this. As you run your periodic Scan Disk function, make note of the lost segments. They are the little black spots on the drive map. They will invariably start increasing and become a precursor to disk failure. Once gone, it is truly over. Recovery of the remaining data can be time consuming and/or expensive.

Now, where is a good place to put this data? You can use a CD, a DVD, a tape drive, an Iomega zip drive, or variations of the USB thumb drive. There are also network drives, internet services and removable drives. The techniques are many and varied.

Dennis McGillis demonstrated a rather neat removable hard drive arrangement. A case (cabinet, container?) is inserted into one of the available access holes on the front of most computer towers. A suitable hard drive is inserted in the case, much like the action we think of for a CD drive insertion. The removable drive can be stored in a safe, fire-proof, of course; a safe-deposit box; or in your car. Safety is the issue.

One person present had everybody excited as he related his offer of a free web service where his clients could access and store back up data. Several people reacted favorably until he emphasized "his clients." He was a computer service person. What a nice way to insure a degree of loyalty from his customers -- particularly considering his business. Nobody likes the repair guy for long.

A CD is particularly helpful if you have a drive on your laptop. However!! Don't leave the CD parked in the laptop drive. We were advised that last year alone, 318,000 laptops were stolen, most of them at airports.

Last but certainly not least, employ an imaging program such as Norton's Ghost. Ghost allows you to re-create your hard drive, programs and all, on another hard drive. Utilize a second computer, usually reserved for this purpose, rather than two drives in one computer. It seems obvious but if the computer is damages by fire, theft or the so-called Act of God, you have no protection with two drives in one box.

We recognize the challenge when setting up such a meeting. Some target topics were all but forgotten as the allocated time made its persistent march toward the closing point. We will see more, we are certain. We are dealing with very busy people who are paid by the second, not the hour. That second is the one when the customer gives the rep an order. All the rest of their time is development time and when spending it sitting in a conference room, it is sometimes hard to recognize what is developing.

Two good hours here could save ten down the road in improved efficiency. For that reason alone, we would have like to have seen more time available. Were we glad that we were given the opportunity to be there? Not yes but, H* yes! Let's do it again, guys.**

HARRISON FRANK AND GUEST CHATTING