The Net Result

TC Lawton

SUPERHIGHWAY SECURITY

This article is intended as a guide to the jargon challenged librarian who has to come up against the computer services department/manager and doesn't have any knowledge upon which to base their struggle to have Internet introduced to at least part of the organisation. Many computer people who themselves have little knowledge of the Net are generally wary of its introduction because of the dangers inherent in opening up any internal networks to external dabblers. It will also serve, hopefully, to help the reader understand some of the issues a bit more clearly. Unfortunately it can only touch briefly on the issues.

The Internet has brought to the masses the opportunity to communicate with a huge number of individuals, mainly unknown to the user, in a variety of formats (eg. Email, IRC, newsgroups), instantaneously (or so it would appear). The key to this is the word "unknown", for although we have gained immense flexibility in the way we now communicate in this global arena, we have also become much more open to potential electronic dangers.

In many ways the cybersociety is open to many of the crimes and problems inherent in normal society with the only differences being in the methods, scale and detectability. The first is interesting to examine from a purely esoteric viewpoint, simply to be amazed at how people can use such a seemingly innocuous technology (to the layperson) to commit the strangest (and most mundane) of crimes. It is however in the second and more importantly third points that cybercrime becomes at least as annoying as its regular counterpart, if not more dangerous.

There are a number of ways to minimise your risk upon deciding to join the global network and, although it must be stressed that there is no way of making your systems totally secure AND keeping them linked to a network, you can at least take precautions and not make mistakes based on naive or uninformed decisions and/or assumptions.

It was best said by Gene Spafford, "*The only system which is truly secure is one which is switched off and unplugged, locked in a titanium lined safe, buried in a concrete bunker, and is surrounded by nerve gas and very highly paid armed guards. Even then I wouldn't stake my life on it.*"

Whilst this may seem overdone it does highlight the important fact that your computers become at risk the minute you connect the power, it is not just a symptom of the Internet that brings potential disaster to your data: it is a by-product of using computers in general. It is fair to say that simply connecting to the Net with the intention of taking information from it (as opposed to supplying information to others) will not provide a great security problem at all. If you only run client software on machines such as Macintosh or Windows, the risks are minimal. In this category the only problems are those of nuisance value, with the potential for bigger disasters if you make errors of judgement. For example, although it is highly improbable that viruses will be loaded and executed onto your machine via Email, they *can* be loaded as an attachment to Email, however you would need to physically run the attachment. The rule of thumb says "Never load or execute anything that comes unsolicited via any source from people you don't know (and even if you do know them make sure you know what you have been sent *before* executing the files)". Commonsense to many but fatal to many more.

In terms of nuisance value, simply having an Email address can prove to be problematic. This is especially true if you have joined one or more mailing lists, identifying yourself as being interested in a particular subject. The key here is that most mailing lists are not secure environments and the entire list of subscribers to a mailing list can often be obtained by automatic means in a matter of minutes by anyone who cares to enquire. Once you have been identified and start receiving junk mail via this method the only effective way to prevent it is to change your address (and not provide a forward). Such a move can be a considerable burden because it means no-one will know how to contact you, so remember to be careful as to what list you subscribe (and remember to unsubscribe when you are no longer interested) and to whom you give your address. (While the author does not believe sending junk mail I a crime per se, it is certainly unsocial behaviour).

The same is true of Email based harassment (although this one is a definite crime). Once someone has your address your only avenue is to install some filtering software to automatically discard mail from a particular sender, or to change your address. In either case you should report the matter to a couple of sources: the postmaster of the offending site (eg. If the offender is fred@foo.com, then report it to postmaster@foo.com), and the federal police. With most cases of cybercrime the federal are a good place to complain/report the problem.

To Be Continued . . . .