COMPUTER SECURITY

A Focus on School Computer Security

Introduction

Though most American schools now have computers and other forms of technology available for use by staff and students, the security attached to these tools is not always adequate. Just as uninformed members of the educational community think that purchasing and installing computers makes their students technologically literate, members of the same community often fail to realize the steps that must be followed to insure the safety of the investment. The following is a list of ten of the most common school site security concerns with comments about the complexity and cost of resolving them.

Security Concerns

#1 – Password security
#2 – Network port security
#3 – Security of student accounts
#4 – Virus protection
#5 – Data backup
#6 – Regular in servicing on security procedures
 # 7 – Physical security
#8 – Climatic Conditions
#9 – Inventory control of software and hardware
#10 – Decommissioning of Obsolete Equipment

Comments and Suggestions

Many of the security problems at school sites such as mine would be reduced if regular staff and student in servicing on security procedures was held on a regular basis. Most people on my staff are not aware of the security problems. Most people are not aware of district security policies or of their own role in any district security plan. Clearly stated policies and procedures provided through regularly scheduled in servicing is a must!

Some steps toward a more secure technology system are fairly simple. For example, in most cases, login names and passwords were assigned and have not been changed on a regular basis. Each user should have a unique password, which they change. That password should keep unauthorized users out of not just district maintained files, but also all of the files on a user's site. Passwords should not be shared. Regular reminders to update passwords cost nothing but a little time. At minimal cost and with a small investment of time, each user would be able to secure his or her files.

Staff needs to back up information on a regular basis, not just at the end of the year. Again, that files should be backed up to a server that is configured so that other teachers or administrators do not have access to files. Disgruntled employees or unauthorized "visitors" could easily destroy curriculum and other materials that are not secure.

The physical setting in which hard and software is kept is very important. Often computers and related hardware are placed in a classroom with an old alarm system. The technological components are merely placed on a table or desk. It is easy for thieves or vandals to access the equipment. In addition, the climatic conditions within the room are important. Electronic equipment is easily damaged by contaminants in the air. Given the lack of cleanliness in some classroom, technology (in addition to teachers and students) is sure to suffer!

School air quality information

Schools invest a great deal of time and money in the installation of computer technology. At relatively low cost and with only a small amount of additional commitment of time, the investment will operate in a more secure environment. Publicizing and enforcing clearly stated policies will put most districts on the road to greater computer security.