COMPUTING WITH CLASS

Security Begins at Home

When you buy a computer for your school, the salesman tells you that it will save you time and money by computing and maintaining student grades and attendance records. Its word processor will make composing test questions easier. In addition, the same computer will teach students how to program, keep track of tuition payments, and maintain records on disciplinary actions—all at the same time—simply, quickly, and efficiently.

At this point, some skeptical teacher or principal is probably muttering, "This all sounds too good to be true." Unfortunately, it is.

When the computer says that Johnny got an "A" in your class when you gave him a "D"; when Mary seems to know what questions were going to be on the midterm even before the copy machine cooled off; and when Bobby's disciplinary record seems suspiciously clean, you may begin to wonder how much of a help the computer really is. If your records and grades aren't secure, what good is it?

Don't despair! Even if someone has cracked your security system, you can still rearm it to prevent future access. Of course, teaching computer ethics would also be a helpful adjunct to resecuring the system. Listed below are some suggestions for ways you can put a stop—right now—to unauthorized access to your computer system.

Add Infinity to Your Routine

If your password has eight characters, then program the computer to demand the first three characters within the first second and wait at least two seconds before accepting the next character. The final characters, which must be entered within two seconds, follow a three to five second wait. The timing can be adjusted or changed periodically by your security programmer. Most students will be frustrated to find that after they have tried every possible combination of eight characters they still can't gain access to the computer.

This procedure alone will keep the casual code cracker at bay. But what about the over-the-shoulder "I can't believe I saw the passcode being entered" threat?

Tie Your Password to a Formula

Most computers maintain an internal clock; some also keep track of the date. If your fixed passcode is 1E7, you could add the military hour in front and the day of the month behind—producing a passcode for 3:30 p.m. February 17 of 151E717. This passcode is only good for one hour, so whoever looked over your shoulder had better hurry.

Still, someone might know your computer's modem number and randomly stumble across the right combination at the right time of day. Or the principal's secretary might share the formula with her boyfriend, the computer whiz. To thwart these threats, you might consider an additional precaution.

Don't Call Me, I'll Call You

Most timesharing systems deal with a limited number of terminals which can be identified and authorized prior to their usage by the telephone number from which you will be dialing. When an authorized person wants to get on-line, he or she calls in as usual, enters the assigned passcode, and waits. Your computer checks the passcode and disconnects the phone. If the passcode doesn't clear, your computer security has not been breached. If the passcode does clear, your computer then calls the authorized terminal. The personnel there may be a little surprised to learn that they called for access to the computer, but no security problem has resulted since the computer did not reconnect to the phone modem at the unauthorized location.

The above suggestions can be incorporated simultaneously. However, they will offer little security protection if you or others on the staff advertise the secret code. That's exactly what you do when you stick your passcode in your top desk drawer, scribble it on your memo pad, or leave it in some other easy-to-find place. It is better to take the time to memorize your passcode than to jeopardize the entire system.

Timesharing users observe the common courtesy of removing themselves from a line-of-sight to the keyboard whenever a passcode is being entered. If you're in the company of potential timesharers who have not been well-bred, do

(To page 34)

Computing With Class

(Continued from page 28)

not enter your passcode until you are sure that they cannot observe you doing so. This isn't a matter of trust; it's a matter of security.

In addition, it makes good sense to be careful to lock rooms where computers are located and to limit access to areas containing terminals or disk backup. Many computer dealers offer locking mechanisms to prevent theft of equipment and hardware.

Remember, it could be a lot easier to prevent a theft or security breach than to figure out what to do about it after it happens.—Dave Ruskjer. □

The author is publisher of *The Journal of AMCA (Adventist Microcomputer Concepts and Applications).*

Separate Articles Removed

Separate Articles Removed