How to pick a practical password

If you want to avoid eighty percent of computer invasion headaches (according to the U.S. Department of Energy's Computer Emergency Response Team Coordination Center at Carnegie-Mellon University), choose good passwords and protect them.

Here are some considerations in password selection:

Make it long--at least 8 characters. The longer it is, the more difficult it is to crack. It is no mistake that some of the online vendors that issue passwords tend to be fifteen or more characters, and Microsoft product security keys may be twenty or more characters.

Keep it fresh. That means changing it every 3 months or more often, every time someone leaves the firm, and, especially, if you suspect invasion or if you know of someone angry enough to attack. Attack tools are easily available on the Internet and many are menu-driven so that all one needs is the emotion-the anger-to set up an attack.

Mix upper case (capital) letters, lower case (small) letters, numbers, and punctuation in your passwords. (Certain punctuation marks cause problems that we will note later.)

Make it easy to remember. Use a phrase you remember and pick one or two letters from each word or use two words joined by a punctuation mark.

Make it easy to type quickly-preferably without looking at the keyboard. If you suspect people are watching you type, be aware of what is going on around you and position your body or some other implement as a block to that line of sight. If you suspect that your password has been compromised, change it as soon as possible.

There are a number of punctuation marks that may cause problems in passwords because in some operating systems, they have special meaning. Since the Internet brings a number of operating systems together that are not always compatible, you are likely to encounter frustration for

reasons not apparent to you if you use one or more of these punctuation marks in passwords. The "at" symbol (@) and the hash symbol (#) mean "erase" or "delete" for some versions of the UNIX operating system and, since the Internet was originally UNIX-based, those symbols can create problems. For the same reason, leading or trailing hyphens create problems because they are used in some UNIX commands. (But embedded hyphens are permitted.) The dollar sign ($) signifies a variable in some versions of UNIX commands and programming. Forward slashes (/), pluses (+), and periods (.) create authentication problems for some systems.

Do not use anything that can be associated with you. That includes your name, address, any identification number associated with you, any family name, or anything else that can be discovered easily about you. Run a complete online search on yourself and make sure that you exclude anything you retrieve and anything relating to anything you retrieve from your password-selection universe.

Do not assume that use of a word in a foreign language will protect you--either forward or backward. The hacker tools test for all of those combinations automatically.

Finally, do not write you password on a sticky note and place it on the frame of your computer screen. That is a disaster waiting to happen.