CREATING STRONG PASSWORDS

This newsletter is one in a series that provides general information on key components of the HIPAA Security Regulation. More detailed information and policies are available on the MCW HIPAA website. In this newsletter we’ll cover methods for Creating Strong Passwords.

We are more technically savvy today than ever before. We bank on-line, shop on-line and typically have several e-mail accounts. For each of these services you have a unique, individual and very likely closely-guarded password. Similarly, MCW passwords are used to restrict unauthorized access to important College information and sensitive data. Your MCW passwords are the “key” to the College’s most valuable information and therefore must be protected.

Today, a stolen password can be used to launch an attack against another system, allow access to a system where a back door might be installed for future use and other felonious acts.

Studies have shown that it is highly likely that the passwords you are using today are inadequate. Several methods can be applied to create stronger passwords - ones less likely to be guessed or hacked.

HOW DO I SELECT A STRONG PASSWORD?

DO. . . use passwords that are at least 6 characters long. Shorter passwords are subject to compromise. Use alpha/numeric characters utilizing upper case and lower case letters, numbers, punctuation and symbols. The key is total randomness.

DO. . . create your own abbreviations. The oddity of your password makes it more difficult for someone to guess or crack. Create your own phrases instead of single words. In fact, it’s best to avoid recognizable words completely. Use odd spellings, i.e., “O2BGophng.”

DO. . . change your password at least every 120 days, per MCW instruction. Passwords are only allowed to be used once within a 12 month period.

DO. . . change any temporary passwords immediately at the first log-on.

DON’T . . use passwords based upon personal information that can be easily guessed, i.e., passwords the same as the userID, your name spelled backwards, children’s names, etc.

DON’T. . . use dictionary words or proper names. The average password cracker program can guess 65,000 dictionary words per second. Also, password cracking programs often can manipulate small details to snag simple attempts at individualization, like using common words followed by a number.

DON’T. . . write your password down or share it with anyone – INCLUDING CO-WORKERS. The password thief knows to look for post-it notes which might be placed under your mouse pad, computer keyboard, on your calendar and even in your Rolodex. Studies show that users frequently hide their passwords this way.

DON’T. . . include passwords in any automated log-on process (e.g. stored in a macro or function key).

DON’T . . forget your password. One of the risks associated with a stronger password is the human factor of memory.

Remember, passwords are pointless if they are easily guessed. Be creative. Be clever. You are solely held accountable for your account access. No one other than you should know your password!

If you believe your password has been compromised, change it immediately. Once done, notify your Systems Manager or contact Information Services at 456-4357.

COMPUTER SECURITY TIP:

PEOPLE SOMETIMES STORE PASSWORDS, PERSONAL IDENTIFICATION NUMBERS (PINS), AUTHENTICATION CODES AND SENSITIVE INFORMATION ON THEIR PERSONAL DIGITAL ASSISTANTS (PDA). IF YOU STORE SUCH SENSITIVE INFORMATION ON YOUR PDA MAKE SURE TO PROTECT THE DEVICE WITH A STRONG PASSWORD!

YOU CAN REFERENCE ADDITIONAL INFORMATION ON COMPUTER SECURITY AT:
The MCW HIPAA website: http://infoscope.mcw.edu/display/router.asp?docid=8598
The MCW Information Services website: http://infoscope.mcw.edu/display/router.asp?docid=7798