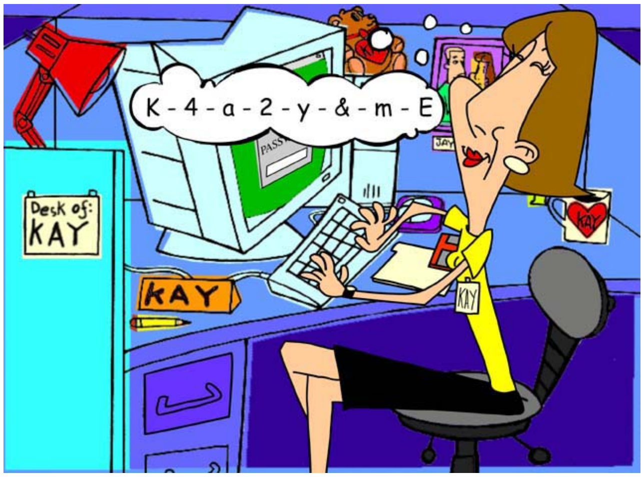
FCC Computer Security Notice

JULY 2002

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, FCC passwords are used to restrict unauthorized access to important Commission information and sensitive data. Your FCC passwords are the "key" to the Commission'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, its best to avoid recognizable words completely. Use odd spellings, i.e., "O2BGophng."

DO. . . change your password at least every 90 days, per FCC instruction. Passwords are only allowed to be used once within a 12 month period.

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, proper names or curse-words. 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. 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. Statistics show that one in 25 users hides their password this way. Don't worry, if needed your manager can request a password change from the Computer Resource Center (CRC) if a file contained within your account is required for use and you are unavailable.

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 immediately change it. Once done, notify the Computer Resource Center at (202) 418-1200 and the Computer Security Officer at (202) 418-1817.

COMPUTER SECURITY TIP OF THE MONTH:

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 the FCC Computer Security Program at:

http://intranet.fcc.gov/omd/itc/csg/index.html

http://intranet.fcc.gov/docs/omd/itc/csg/response-team/ia.doc