HOW TO CREATE “STRONG” PASSWORDS

Strong passwords are important because passwords are often used as the first line of defense against unauthorized access.

Many users find passwords to be a hassle and don't heed recommended passwords do's and don'ts. Accordingly, some of the biggest DON’Ts with regard to passwords are: password sharing, using common names such as your spouse, children, and pets as your password, sending your password in a clear text form, creating passwords that are too short, creating passwords that are all alphabetic or all numeric, or using the same password for all accounts.

For convenience sake, most users would like to pick one password, and 1) use it for all of their accounts, 2) use it all the time, 3) never have to change it, and 4) write it down so that they can reference it if they happen to forget it. However, the problem is if the password is easy to remember, it is easy to guess. If the password is written down, guessing doesn't even matter. And if the password is never changed, then repeated attacks are more likely to occur.

Experts recommend the following tips to help you select a password that is more secure, yet still relatively easy for you to remember:

Use a minimum of 8 characters.

Don't pick a password that someone can easily guess. What types of things are easy to guess? Here's a list of things that you should not use because they are easy to guess.

- *Don't use your login name in any form (as-is, reversed, capitalized, doubled, etc.).*
- *Don't use your first or last name in any form.*
- *Don't use your spouse's or child's name.*
- *Don't use other information easily obtained about you.* This includes license plate numbers, telephone numbers, social security numbers, the brand of your automobile, the name of the street you live on, etc.
- *Don't use a password of all digits, or all letters.* This significantly decreases the search time for a cracker.
- *Don't use a word contained in (English or foreign language) dictionaries, spelling lists, or other lists of words.*

Use a combination of numbers (1-9), alpha characters (A-Z), combination upper case/lower case, and special characters (!, @, #, $, %, ^, &,*,+,=). For example:

Get>Sm@rt

If it is hard for you to remember special characters, create a common substitute that makes sense to you. For example, use $ as a substitute for s or S, @ as a substitute for A or a, (or [as a substitute for C or c, or + as a substitute for t or T. So instead of *Get>Sm@rt*, the password could be *Ge+>$m@r+*

Use a passphrase

A passphrase is sort of like a personal algorithm. The phrase makes it easy for you to remember, but hard for someone else to guess. For example: The title of the song *I Left My Heart in San Francisco* is a phrase that could be represented by the following password: eyeLMHi$F If you like the idea of using memorable information in a passphrase that will make no sense to someone else, consider the following passwords:

4$@$y@rfbfo+[@nn

Four score and seven years ago, our fathers brought forth on this continent a new nation

@nwy[[d4u@wu[d4y[

Ask not what your country can do for you; ask what you can do for your country.