

## Password Selection Guidelines

### *Why should you care about compromising your password?*

A compromised password can easily be used in ways that you are unlikely to notice, such as remotely reading your email. Keep in mind that a poorly chosen password not only places all of your own files and data at risk but also places your colleagues and co-workers at increased risk by allowing an outsider to masquerade as you and avoid all restrictions normally in place for external access to the environment. Thus, it is never reasonable to keep an easily guessable password on your account simply because you are willing to personally take the risk. Your password is the primary defense against unauthorized access to both your private information and that of the University.

And the risk of compromise is real: Given enough time, any password can be found simply by trying all possible combinations. For example, an all lower case 6-character password can be found in about 4 days by brute force search on a machine that can try 1000 passwords per second.

However, for well-chosen passwords a brute-force attack is still infeasible even using today's fastest computers, as long as you change passwords from time to time and as long as you follow a few basic guidelines.

### **Do's and Don'ts for selecting a password**

- *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 the same letter. 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.
- *Don't* use a password shorter than six characters.
- *Do* use a password with mixed-case alphabets.
- *Do* use a password with nonalphabetic characters, e.g., digits or punctuation.
- *Do* use a password that is easy to remember, so you don't have to write it down.
- *Do* use a password that you can type quickly, without having to look at the keyboard. This makes it harder for someone to steal your password by watching over your shoulder.

Although this list may seem to restrict passwords to an extreme, there are several methods for choosing secure, easy-to-remember passwords that obey the above rules. Some of these include the following:

- Alternate between one consonant and one or two vowels, at least 6 characters. This provides nonsense words that are usually pronounceable, and thus easily remembered. Examples include “routboo,” “kuadpop,” and so on.
- Choose two short words and concatenate them together with a punctuation character between them. For example: “dog;rain,” “book+mug,” “kid?goat.”

For help with any password related problem or if you have questions please call the ITS help desk at (706) 737-1482

### **Password Maintenance**

Once selected, your password should not be recorded anywhere either on paper or in a computer file.

Do not share your password with anyone. Anyone who needs access to the system will be given their own account.

Change your password regularly. Every 90 days is a good suggestion for regular changes.

These guidelines are intended for your protection by making both your account and the University computer systems more secure.

If you believe that your password has been compromised and that your account is being used by some other individual, please call the ITS help desk at (706) 737-1482. Action will be taken to monitor the account and any intruder will be discovered and prosecuted.