How Good Is Your Password?

UFIT

2046 NE Waldo Rd, Suite 2100
Gainesville Florida 32609-8942
(352) 392.2061
<editor@cns.ufl.edu>
# Table of Contents

How Good Is Your Password? ................................................................. 3  
Selecting Passwords ....................................................................... 3  
Do: ................................................................................................. 3  
Don't: ............................................................................................. 3
How Good Is Your Password?

Adapted and reprinted with permission from InfoTalk, newsletter of the Emory University Information Technology division, January/February 1992.

How would you feel about a computer "hacker" prowling through your files, reading them and perhaps changing them or sending offensive messages using your ID and name? Or perhaps a coworker who's curious about what files you have or wants to use your ID and computer accounts? There are people out there who consider it challenging and fun to break into someone else's computer. One of the common methods is to guess your password by using a list of common words or names found in an online dictionary.

Selecting Passwords

The objective when choosing a password is to make it as difficult as possible for a cracker (computer "hacker," unauthorized intruder) to make educated guesses about what you've chosen.

The proliferation of high-speed desktop CPUs makes it necessary that your password also be as safe as possible from brute-force searches, where every possible combination of letters, numbers and punctuation is attempted. With this as our goal, a set of guidelines for password selection can be constructed.

Do:

- Use a password with mixed-case letters upper and lower case on NERSP (NERDC's other systems are not case sensitive with regard to passwords).
- Do use a password with nonalphabetic characters; e.g., digits or the special characters #, $, or @.
- 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 looking at the keyboard. This makes it harder to steal your password by watching over your shoulder.
- Do use as many characters as allowed by our systems (currently eight). Longer passwords are much harder to crack than short ones.

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 car, the name of your street, your pet's name, etc.

• Don't use a password of all digits, or all the same letter. This significantly decreases a cracker's search time.

• Don't use proper names, or characters from works of fiction, or team names such as "Gators."

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 -- but don't use any of these examples! They're well known and easily cracked! Consider them as samples only.

Choose a line or two from a song or poem, and use the first letter of each word. For example, "If you want to be happy" becomes "Iywtbh."

Alternate between one consonant and one or two vowels, up to eight characters. This provides nonsense words that are easily pronounceable, and thus easily remembered. Examples are "routbou," "quadpoup," and so on (but avoid doubles of any letter or word).

Choose two short words and concatenate them together with a number or special character between them. For example, "dog3rain," "hook$mug," "kid7goat."

The importance of observing these password selection guidelines cannot be overemphasized.

Your Comments are Welcome

We welcome your comments and suggestions on this and all UFIT documentation. Please send your comments to:

UF Information Technology

UFIT

2046 NE Waldo Rd, Suite 2100
Gainesville Florida 32609-8942
(352) 392.2061
<editor@cns.ufl.edu>