## What is a Password?

It is a secret combination of letters and numbers that verifies your identify to the computer.

## Remember the following two principles

***Protect your password.***

Don't write down your password - memorize it. In particular, don't write it down and leave it anywhere, and don't place it in an unencrypted file! Use unrelated passwords for systems con-trolled by different organizations. Don't give or share your password, in particular to someone claiming to be from computer support or a vendor. Don't let anyone watch you enter your password. Don't enter your password to a computer you don't trust or if things Use the password for a limited time and change it periodically.

***Choose a hard-to-guess password.***

On Unix/Linux passwd will try to prevent you from choosing a really bad password, but it isn't foolproof; create your password wisely. Don't use something you'd find in a dictionary (in any language or jargon). Don't use a name (including that of a spouse, parent, child, pet, fantasy character, famous person, and location) or any variation of your personal or account name. Don't use accessible information about you (such as your phone number, license plate, or social security number) or your environment. Don't use a birthday or a simple pattern (such as backwards, followed by a digit, or preceded by a digit. Instead, use a mixture of upper and lower case letters, as well as digits or punctuation. When choosing a new password, make sure it's unrelated to any previous password. Use long passwords (say 8 characters long). You might use a word pair with punctuation inserted, a passphrase (an understandable sequence of words), or the first letter of each word in a passphrase.

These principles are [may be] partially enforced by the system, but only partly so. Vigilence on your part makes the system much more secure.

# Important for Security

## Awareness

Passwords are the front door.

Passwords serve as a security measure against unauthorized access to data. However, the computer can only verify the legitimacy of the password, not the legitmacy of the user. The weakness of passwords is that they can often be forgotten, stolen or accidently revealed.

## Response

What must you do? You must buy into the need to use passwords and use them correctly. You have to understand and accept that passwords are important, necessary and effective. This requires discipline and working with the inconvenience of using good passwords.

## Why do passwords matter?

Most systems are cracked (broken into), root (unrestricted administrator level) access gained, by means of using a normal user account.

## User Responsibilities:

***Do not share user accounts.***
***Select a good password and keep it private.***
***Log off when not using the computer system.***
***Use file permissions on files and directories (folders).***
***Notify System Admin if password compromised.***

## System Administrator Responsibilities:

***Teach Users***
***Teach Management (Users that set policy)***
***Secure The System***

# Consider these items:

## *1990: Estimated Discovery Time*

Eight (8) characters, [uppercase letters and digits only] making 2,800,000,000,000 possible combinations, would take ***890,000 years*** to break.

## *2001: Estimated Discovery Time*

Eight (8) characters, [uppercase letters and digits only] making 2,800,000,000,000 possible combinations, would take ***10.7 months*** to break.

## *2005: On length of Password*

"A password should be at least 10 characters [mixed case, digits and punctuation] long..."
Bob Toxin, Linux Security, Insecure Magazine, pg 17, April 2005

## *2005:Estimated Discovery Time*

Oracle password hashing: Eight (8) characters [uppercase letters and digits only] in 39.3 days [Estimated discovery in ***20 days***] using a standard Intel Pentium 4 2.8 Ghz workstation.

*http://www.sans.org/rr/special.php*

# Good Passwords

## How to Choose a Good Password

*Understand problems.*
*Avoid common mistakes.*
*Make them easy to remember.*

## Guidelines:

**1 Don't use passwords that consist of easily obtainable personal information, such as your address, phone number or date of birth. Also avoid using common words found in a dictionary.**

**2 Devise passwords of at least eight characters consisting of upper and lower case letters, numbers, and symbols, for example: WEle@rN?.**

**3 Use a different password for computer system or each service you register with.**

**4 Ideally, a password should be easy to remember. However, the reality is that having multiple passwords becomes confusing--which password is for which site? If you need to record your passwords, store them in a secure location. A piece of paper in the top drawer of your desk is tempting fate. Even worse is a Post-It note on your monitor.**

**5 Never disclose your password.**

**6 For sensitive accounts, such as financial services, change your passwords frequently. We recommend every two months.**

## Bad Examples:

*xyzzy - secret words from games, movies, books*
*240HIK - my vehicle license plate*
*Winston - names, unusual or otherwise*
*sweetpea -name of pet, person, project*
*Sony15sf - monitor on my desk*
*qwerty123 - keyboard sequence*

## More Bad Examples:

*mx1234z - too short (should be at least 8 )*
*sections - word in dictionary*
*snoitces - reversed dictionary word*
*secrets3 - dictionary word with number tacked on*
*53cti0n5 - word with 5 for s, 3 for e, 0 for o*

## Good Pass Phrase Examples:

*2Old4U2c - License plate vanity style - memorable*
*Ott4fss8 - One,Two,Three,4,Five,Six,Seven,8*
*Nwh4iie8 - oNe,tWo,tHree,4,fIve,sIx,sEven,8*
*itMc?GiB - is that My coat? Give it Back*

## Better Pass Phrase Examples (Longer is Better):

*2Embp,1ib - 2 Elephants make bad pets, 1 is better*
*Mrci7yo2d! - My rusty car is 7 years old 2 day!*

## Resources:

Password Guidelines:
*http://security.fnal.gov/UserGuide/password.htm*
Password Security- A Sample Guide:
*http://www.umich.edu/~policies/pw-security.html*
Password Guidelines - A Policy Example
*http://www.microsoft.com/ntworkstation/technicalresources/PWDguidelines.asp*
Security Password Guidelines- Another Example
*http://www.tcnj.edu/~it/security/passwords.html*
Guidelines for choosing a good password
*http://www.lockdown.co.uk/?pg=password_guide&s=articles*
GeodSoft How To: Cracking Passwords Techinques
*http://geodsoft.com/howto/password/cracking_passwords.htm*
Password Recovery Speeds - How Long Will Your Password Last
*http://www.lockdown.co.uk/?pg=combi*

# An introduction to Passwords:

## the keys to let authorized users work, keeping others out.

# Password Guidelines for Beginners

**Brought to you by the**

## St. Louis Security Group

***www.sluug.org/security***

***A Special Interest Group of the***

## St. Louis Unix Users Group (SLUUG)

***www.sluug.org***

The Security SIG meets on the 4th Wednesday of most months Start time is 6:30 PM, stop time is 8:00 PM, out by 8:30 PM. Sessions usually include Hands on Lab using both Microsoft Windows XP and Unix (GNU/Linux) PC workstations. The UM-St. Louis Microcomputer Program provides the training lab rooms and computers for these hands-on sessions. These facilities are at the West County Computer Center near Interstate 270 and Manchester Road at 1710 Deer Tracks Trail, Suite #240, St. Louis, MO 63131.



***April 2006 version 0.4***