



How to Choose a Secure Password

What is a secure password?

A **secure** password is at least 8 characters in length, it not a single word (backward or forward) found in any dictionary (English or foreign language), and it does not contain any personal information someone could discover about you, such as your name, username or ID, or the name of a family member, your address, birthday, anniversary date, phone number, social security number, brand of automobile, or favorite pastime.

It must contain a combination of numbers and letters with the numbers in the middle of the password because cracking programs will attempt numbers at the beginning or end of a password. Refer to the example of a secure password below:

|Anatomy of a Secure Password

Mixed numbers and letters...*

Upper and lower case

Mixed8UP

*...or other characters as allowed by your systems administrator

MINIMUM of 8 characters



Why is it important?

Internet worms have the ability to “guess” weak passwords and password “cracking” tools are widely available.

Someone with any of the 72 cracking programs (recently counted on a hacking site) can crack against English and foreign dictionaries, forward and reverse spellings, slang (like BRB, TTYL, LOL, or time2go), all numeric entries, numbers at the beginning or end of a word, or numbers substituted for similar letters in words (like PAS5W0RD), at the rate of 216,000,000 crack attempts per day.

The bottom line:

Someone with a cracking program can break into a computer with a weak password in less than an hour.

How to choose a secure password

Step 1: Follow the mnemonic **Mixed8UP** (see ***Anatomy of a Strong Password***, previous page):

- **Mixed** characters (letters and at least one number in or near the middle)
- **8** characters (minimum)
- **UPPER** and lowercase characters

In addition, please be sure that your RIT account password:

- Is not a single word (forward or backward) in a dictionary (English or foreign), even if you have substituted a number for a letter (like “5” for S).
- Does not contain your username or user ID
- Does not contain consecutive repeating characters
- Is changed at least every 120 days or whenever a virus is detected or you suspect your computer has otherwise been compromised
- Is different from the password you use on your home computer or for other applications or web pages
- Is changed if you (or someone who works for you) change jobs
- Is not one of the examples from this or related documents on changing your password.

Step 2: Once you have chosen a secure password, follow the password change instructions for your computer. This applies to administrator passwords as well. (Contact your systems administrator for assistance, if needed.) For example, use the ITS password change utility at <http://start.rit.edu> for your RIT account (formerly known as DCE).

Step 3: Keep it secure. Don’t share it with anyone for any reason.

A hard to guess password is not hard to remember

- You can use the first letter of each word in a favorite quotation, book title, song, or poem, and add a number in the middle. For example, the quotation “*Imagination is more important than knowledge*” by Albert Einstein could become “**iimitk8AE**,” or “**iimitk1AE**.”
- Alternate between a random consonant and vowel to produce a nonsense word that can be pronounced. For example, “*hikupwaso*.” Now add a number. For example, “**hikup8WASO**.”

- Choose two shorter words and put them together with a number in between. For example: “b**OOK**451**BRAD**bury.”

Write it down and store it in your wallet

An effective password may initially be harder to remember, so go ahead and write it down and store it in your wallet with your other valuables. Please **DO NOT** write it on a post-it note or calendar near your computer where someone can walk up and find it.

Where to go for more information

The Information Security web site at <http://security.rit.edu> contains more sound security practices related to passwords. The Security Standard – RIT User Account Passwords can be reviewed at: http://security.rit.edu/standards/passwordstandard_Users.pdf and the associated sound security (Best Practices) can be reviewed at http://security.rit.edu/bestpractice/securepassword_bp.pdf.