

# *Password Best Practices*

**Author:**  
Razorpoint Security Team

**Version:**  
1.5

**Date of current version:**  
2006-05/01

**Date of original version:**  
2001-04/04

**Copyright © 2001-2006 Razorpoint Security Technologies, Inc.  
All Rights Reserved.**

ISIT?  
SAFE<sup>SM</sup>

## Password Best Practices

One of the most overlooked areas of network security is the use of "good" passwords.

Extreme care should be taken in choosing your password. If your password is easy to guess, someone may be able to access or steal your data, your money, or your identity. To protect your data, your network, and yourself to some degree, you must select good passwords and secure them carefully.

Users are responsible for assisting in the protection of the systems they use. As an Internet security measure, computer and network passwords should be changed regularly. Additionally, the use of different passwords for different systems is recommended so that if an intruder cracks one password and gets into one computer, that same password won't automatically allow access to other systems.

Choosing good passwords can be thought of as more art than science. Criminal hackers (a.k.a. Crackers) have tools that can break any password (or modified facsimile) found in a dictionary. Password guessing and dictionary attacks (cracking) are common ways of gaining unauthorized entry into networks, and even the best passwords can eventually be defeated mathematically, given enough time. The use of good passwords acts as a deterrent against password guessing and cracking attacks, and can make "brute force" attacks (see The Razorpoint Security Glossary) less successful.

---

The following guidelines outline best practices when choosing, maintaining, and protecting your passwords:

**DO** make sure your password is at least 8 characters long.

**DO** use a password with mixed-case letters, numeric characters and punctuation (where supported by the operating system). Do not just capitalize the first letter, or add a number at the end. The more complex a password, the longer it will take to crack.

**DO** use a password that can be typed quickly, without having to look at the keyboard. This makes it harder for someone to steal your password by looking at your fingers while you type. This is known as "shoulder surfing." (see The Razorpoint Security Glossary)

**DO** change passwords regularly. The more critical an account to network integrity (such as root on a Unix host or Administrator on Windows), the more frequently the password should be changed. This makes your password a "moving target" and makes cracking and brute force attacks less effective. Regular password changes can also stop continued access of an already compromised account. Change passwords at least every six months.

**DO** try one of the following methods for password selection:

**Option 1:** Explore using two words separated by a number or punctuation, like "Pro%F0otball" or "|0n&dog"

**Option 2:** Take a word and change the case on some of the letters. Then, either insert a letter or punctuation, or replace some letters with numbers or punctuation (but avoid common substitutions like a->4, I->1). Even better, use a combination of insert/replace: (Example: bomber -> b0mBer -> b0m&Ber -> %0m&Ber)

**Option 3:** This may be the best option for creating a complex password without having to remember it. Start by choosing an area of the keyboard to use for your password. Next, decide on a pattern for the password. For example, take the upper-left quadrant of the keyboard and create two lines using 2ws3ed3e or, better yet, combine that sequence which shift characters to get 2ws#ED3e. With this method, you don't have to memorize any passwords, you simply have to remember where the pattern starts on a keyboard.

(note: It is a bad idea to use these exact examples as your password). ;^)

---

**DO NOT** use the word "password" as your password, in any form (reversed, capitalized, or doubled). This is not a joke, people actually do this.

**DO NOT** use a network login ID in any form (reversed, capitalized, or doubled) as a password.

**DO NOT** use common names of people or places as a password.

**DO NOT** use keys in a natural progression, like "QWERTY", or "1234", or "abcabc", or "....."

**DO NOT** use a word (forward or reversed) contained in English or foreign dictionaries, spelling lists, or other word lists. These types of passwords are among the easiest to crack. On a moderately fast computer, it is possible to crack a dictionary word-based password in seconds. It is important to remember that generally a computer is doing the guessing, not a human. A computer can be programmed to search through any list of words and try any algorithmic variation. The ways in which users choose passwords are well known to the authors of password cracking programs.

**DO NOT** use words that are acronyms, technology terms, geographical locations or product names (dictionaries for these exist, too).

**DO NOT** use a password of all numbers or alphabetic characters. Mix numbers, letters and punctuation (where supported by the operating system).

**DO NOT** use a password that is simply a word either preceded or followed (or both) by a non-alphabetical character.

**DO NOT** use passwords that match a dictionary word with common "number-for-letter" substitutions.  
 (Examples: a->2, a->4, b->8, e->3, h->4, I->1, l->1, o->0, s->\$, s->2, s->5, z->5, etc.  
 as in: airplane -> 4irpl4ne -> 41rpl4ne -> 41rpl4n3)

**DO NOT** use passwords that are words with vowels deleted, or are made lowercase then reflected.  
 (Example: mechanic -> mchnc, or Super -> superrepus).

**DO NOT** use information easily obtained about you. This includes your first, middle or last name in any form, your initials or any nicknames you may have, spouse or children's names or birth dates, pet names, license plate numbers, telephone numbers, ID numbers, the brand of your automobile (or the one you wish you had), the name of the street you live on, and so on. Such passwords are very easily guessed by someone who knows the user.

**DO NOT - repeat - DO NOT** write passwords on sticky notes, desk blotters, calendars, or store it under your keyboard, under your phone, or online where it can be accessed by others. This is one of the most frequent ways unscrupulous users gain unauthorized access to computer systems.

**DO NOT** use passwords that are so complicated they have to be written down. See above.

**DO NOT** use passwords that you have used in the past.

**DO NOT** share passwords except in true emergency circumstances or when there is an overriding operational necessity. Be sure to change your password immediately after sharing. In an emergency situation, be absolutely certain to whom you are giving your password, and how it will be used. Getting someone to reveal a password by deceit or lying is called "Social Engineering" (see The Razorpoint Security Glossary) and can be very effective in gaining unauthorized access to computer systems. Under normal circumstances a password should never be shared, but if it is, change it immediately after usage.

Password Examples			
Bad Passwords	Description	Good Passwords	Description
<b>mypassword</b>	Two dictionary words together.	<b>T*x4\$M8n</b>	8 characters, uses numbers, punctuation, and upper and lower case letters.
<b>1234567</b>	Repeating sequence.	<b>j@T"PI4Ne</b>	Two words, separated by punctuation, using upper and lower case letters, and numeric substitution.
<b>abcabc</b>	Repeating sequence.	<b>M0ca5V@ca8</b>	Two nonsense words, upper and lowercase letters, and punctuation.
<b>h311o</b>	Less than 8 characters, and based on a dictionary word with common letter/number substitutions.	<b>5tg^YH%TG</b>	Simple pattern that doesn't require memorization. Not based on a dictionary word, uses upper and lower case letters, and punctuation.
<b>test1234</b>	Very common test or default password.	<b>*RUF8ruf</b>	Another pattern with appropriate characters.
<b>admin</b>	Very common default password.		
<b>gandalf1</b>	Based on the name of a popular character.		
<b>john4</b>	Based on the user's name, too short, no upper case or punctuation.		
<b>ydnic</b>	Still a proper name (even though it's backwards), too short, no upper case, numbers, or punctuation.		
<b>PORSCHE911</b>	Proper name, in the dictionary, no lower case, or punctuation.		
<b>Pepsi21</b>	Product name with numbers at the end.		

## Other Password Factoids:

It is important to tailor your password to your system:

- Most UNIX systems will only use the first eight characters of a password. Check your particular operating system.
- Oracle applications such as LETS only allow \$, \_, and # as special characters.
- UNIX passwords are case sensitive, so "password" is not the same as "PASSWORD". Conversely, VMS passwords are not case sensitive, so "password" and "PASSWORD" are the same.
- Use Secure Shell (SSH) (see: [www.openssh.org](http://www.openssh.org)) to avoid sending your password over a network as clear text. SSH encrypts username and password information before sending it over a network. Anytime you type your password to log in to another computer using telnet, ftp, rlogin, etc., your password can be stolen. Crackers can break into networks and steal your password using tools that "listen" for passwords.
- If you suspect your password has been stolen, cracked or compromised in any way, change it immediately.

**For more information on appropriate password use and Internet security, please contact Razorpoint Security Technologies, Inc. at ([www.razorpointsecurity.com](http://www.razorpointsecurity.com)).**