

Choosing Your Password

Avoid The Following 21 Pitfalls:

1. Any part of your name
2. Your account name (this is a hanging offence)
3. Anything less than 7 characters long (system permitting)
4. Any part of the name of a member of your extended family (inc. pets) or, worse, a colleague
5. Name of operating system
6. Significant numbers (phone number, car licence number)
7. place names
8. Favourite or most-hated things
9. easy associations with favourite or most-hated things: for instance "Swan_Lake" is a bad password for a ballet freak
10. Any correctly spelled English word, especially one which is likely to be recognized by UNIX *spell*, application spell-checkers etc.
11. Any correctly spelled non-English word: exceptions may be acceptable in Urdu, any non-Mandarin dialect of Chinese, or Catalan, as long as they're not in languages you're *known* to speak
12. Song-titles, famous people, cartoon characters etc. Particularly avoid 'CharlieBrown', 'Snoopy', 'Kirk', 'Spock', 'McCoy', 'Garfield' and 'Doonesbury': well, you get the idea...
13. Anything so unmemorable you have to write it down
14. Anything which is all upper case or lower case (unless the system is case insensitive!)
15. Anything with the first or last character uppercase and the rest lower case
16. Anything you've come across as a textbook example
17. Anything containing letters of the alphabet only
18. Any significant numeric string, e.g. phone numbers, birthdates
19. Popular choices such as *wizard*, *password*, *today*, *AAAAAAA*, *QWERTYUIOP* etc.
20. Anagrams of any of the above, especially simple reversals etc.
21. Obvious variations such as appending or prepending a digit to one of the above or an anagram thereof

Try These Top Nine Strategies...

1. Interleave two words e.g. Justin Timberlake = JtUiSmTbleNrlake
2. Interleave a word with a numeric string e.g. flash 978 = f9L7a0s8H
3. Concatenate two words, possibly with a symbol as delimiter e.g. egG^rIbBoN (read: egg^ribbon)
4. Embed control characters or non-alphanumeric symbols (!@#\$\$%)
5. Misspell (but consistently!)
6. Unorthodox caPitaliSation
7. Use a personally significant acronym e.g. ICRMPW (I Can't Remember My PassWord)
8. Replace letters with digits or equivalent characters, and words with abbreviations e.g. BunZ4T
9. **Don't use the same password on several machines.** However, sensible variations might be acceptable, subject to the rules mentioned above e.g. VdOOmAX, UdOOMniX, dOoCP/M,

Important Note:

We have given you some techniques that may help in slowing down password breaking by guessing or simple dictionary attacks. Please note that sophisticated crack programs will attempt to counter many of these strategies.

Contributed to the Securing our eCity initiative by:

David Harley BA CISSP FBCS CITP
Small Blue-Green World

Copyright on this document remains with the author and Small Blue-Green World, and all rights are reserved. It may only be reproduced or distributed with the prior permission of the copyright holder and due credit.