WHAT IS A SECURE PASSWORD?

Make your password a secure one. Follow these guidelines.

A secure password

- is at least six but no longer than eight characters
- contains numbers, punctuation and upper- and lower-case letters
- does not contain a colon (:)
- does not contain your user ID or anyone's name, either forwards or reversed
- does not contain any string of characters associated with you (your licence plate, your telephone number, etc.), either forwards or reversed
- is not a word that can be found in any dictionary (English, French, Spanish, biographical, specialized, etc.), either forwards or reversed

A secure password that you can remember easily may contain one or more misspelled or combined words, numbers or punctuation marks (but not a colon). Some examples: brkFst42, OKBlu'Js, Big&gr8. Don't use these examples – invent one of your own.

Change your assigned password the first time you log in. Change it again every three months.

Following these guidelines helps defend you and others from unauthorized use of your account, your files and your computing funds.

THANK YOU
for your cooperation

Security... it's up to you

Satnam Purewal
satnam.purewal@ubc.ca

In 1960, following his study of security in government departments, Lord Radcliffe stated that "the single biggest risk to security is probably a general lack of conviction that any threat exists" (Information Security 15-350-102, May 1992).

This is still true today. Most people feel that they do not need to be concerned about security because they do not have access to anything of interest. I often hear comments like "Why would anyone want access to my account?" Believe me, there are several reasons for being concerned, one of which is the *hacker*. A hacker is "a technically sophisticated computer enthusiast who enjoys...breaking a system's security simply for the challenge of doing so."

If unauthorized access is gained to your account...

The minimum damage a hacker could do would be to sign on to your account and read confidential electronic mail. Depending on the maliciousness of the individual, they may reply to your e-mail or forward it to other potentially interested parties. They may even post copies of confidential e-mail on newsgroups. These things have happened!

It gets worse. If a hacker gains access to your account, they could use it to gain access to other accounts. This can be done by trying to decrypt the password file. Your password is stored in encrypted form in a hidden file. Hackers know that no system is one hundred percent secure and for this reason, hackers have the patience, persistence and resources (thanks to your account) to locate the file. Once it is located, they will try to decrypt the password file.

A hacker may even use your account to post a message fabricating facts about you to an undesirable newsgroup. This could be very damaging to your reputation. As a result, you may be inundated with mail. People who have had such experiences have found them to be time consuming, stressful and difficult to resolve.

> **"the single biggest risk to security is probably a general lack of conviction that any threat exists"**

A hacker may also wish to gain access to a different site. If access is gained using your ID, a hacker may use your account to launch password attacks on remote systems through the UBC campus network. In such cases, your account could be suspended until our system administrators are able to trace the event to the appropriate individual.