IT Security Corner

Password Security

Passwords have been used for centuries. We can all remember reading stories or seeing movies in which gate guards demanded the correct password from people wanting to enter a walled city. Today, passwords safeguard work done on the computer. In this article on security, we will provide you with tips on how to properly construct, protect and maintain secure user passwords.

How to Construct a Secure User Password

Too often users employ passwords that are easy for others to guess; for example, LMXUSER1 or LMXUSER11. Other passwords frequently used by staff include their user ID, own name or the names of family members, friends or even pets. Simply put, employing predictable passwords like these makes it easy for someone to gain access to your account.

For SIGNET, a secure password is eight characters in length, and comprised of alpha, numeric and special characters. A cleverly constructed passphrase, for example, "I am 5'10"" can be condensed to form the easy-to-remember password, "IAM5_10_". Note the use of _ as a special character. Here is another example of a passphrase abbreviated to become a password: "Me for you" becomes the password, "ME_4_U#!". Again, note that this password is made up of three letters, one number and four special characters.

ISSC is often asked if security is lessened by using the same password to login to SIGNET D and ICONDESK. Given the sensitivity of the information which is authorized for SIGNET D, the answer is no. In fact, the same, well-constructed password can also be used for other applications on SIGNET D, such as FINEX and COSMOS.

You, no doubt, have noticed that the system prompts you to change your password every 120 days. What is the reason for this? To increase the security of SIGNET D. In addition, a password history file prevents you from employing eight previously used passwords. This discourages "leap frogging" two favourite passwords.

SIGNET C Passwords

The same password construction techniques used for SIGNET D should also be used for SIGNET C (classified). However, ISSC strongly recommends using a different password for SIGNET C because of the sensitivity levels of information processed on SIGNET C. On SIGNET C, every 90 days the system will prompt you to change your password.

Password Distribution

ISSC discourages the sharing of passwords between users. In fact, one rule we have in our security awareness briefings is: Do not ask someone for their password, and do not offer someone your password.

On a final note, managers are requested not to maintain a list of user passwords. Should you, as a manager, require access to a user's account in his or her absence, we recommend that you contact your System Administrator, who will arrange access for you. This safeguard preserves the security and integrity of an individual's account.

Secur IT Tips

- Develop and use good password construction techniques.
- Commit passwords to memory
- Do not share your password with others.
- Use different passwords for SIGNET C and SIGNET D.
- Do not maintain lists of user passwords.

SIGNET Newsletter is published fortnightly by the SIGNET Client Services Division (STC) and distributed in Canada and at missions abroad to all employees of the Department of Foreign Affairs and International Trade.

Units wishing to have a notice published in the *SIGNET Newsletter* should forward the text to STC with a memo signed at the director level. All readers are invited to send to the SIGNET Suggestion Box draft articles they wish to have published.