IT SECURITY CORNER

SECUR IT

15 Practical Security "Tips" for SIGNET Users

SIGNET-D, the unclassified/designated version of SIGNET, is only authorized for processing, storing or communicating (transmitting) information that is UNCLASSIFIED or PROTECTED. Information which is designated PROTECTED-SENSITIVE or is classified CONFIDENTIAL or higher must NOT be processed on SIGNET-D, as the system does not provide adequate protection for this type of information.

Information transmitted by SIGNET-D is done in the clear; that is, the information is not encrypted. When information is sent from one site to another (e.g., mission to HQ), or is transmitted internally (e.g., workstation to printers), including e-mail, it is unprotected. Even when a SIGNET-D workstation appears to be in stand-alone mode, there are possible network connections; connections to printers, for example. With easily used and readily available programs, it is possible to capture and monitor information, user IDs and passwords on SIGNET-D.

Employees are responsible for the security of information they handle and process on SIGNET. To ensure that appropriate security procedures and precautions are observed, ISSC recommends:

1. Never process classified or PROTECTED-SENSITIVE information on SIGNET-D. Use a TEMPEST stand-alone workstation with a removable hard drive, a non-TEMPEST stand-alone workstation with a removable hard drive (HQ ONLY), SIGNET-C2, DUCS, or Secure FAX instead;

2. Be aware of the security limitations that exist with respect to the processing of critical non-sensitive and sensitive information on SIGNET-D;

3. Include the classification or designation on each message or document processed, stored or transmitted;

4. Label each diskette containing other than UNCLASSIFIED information with the highest designation or classification level of the data it contains. A diskette with PROTECTED-SENSITIVE or classified information should never be used on a SIGNET-D workstation;

5. Recognize that information stored on the hard drive of a SIGNET-D workstation can be directly accessed by individuals without a user ID and password;

6. Protect passwords and ensure that they are changed frequently;

7. Ensure that you logout of your workstation if leaving it unattended;

[A useful complimentary feature to this is the automatic password invocation that can be turned on in the Windows Screen Saver.]

8. Ensure that data files and applications are backed-up and stored separately from the workstation;

9. Verify that diskettes containing sensitive information are destroyed according to established procedures. The delete command does not remove the data, but only changes the file name by removing the first character in the file name. This data can easily be recovered by a knowledgable individual until overwritten by another file;

10. Refrain from and discourage "browsing" through files and programs for which specific access has not been authorized;

11. Ensure that only authorized software is installed on servers and workstations, as the use of unlicensed software (including shareware used beyond its demonstration period) is illegal;

12. Refrain from installing unauthorized modems or connections to other computers or networks;

13. Treat all diskettes from external sources (this includes your co-worker at the next desk and new preformatted diskettes from sealed packages) with caution, as they could potentially be infected by a malicious code. Scan the diskette for viruses before using in your workstation;

14. Ensure that your workstation is scanned regularly for virus infections; and

15. Report all security concerns and security incidents, such as suspected intrusion attempts or virus incidents, to ISSC.

SIGNET Newsletter is published fortnightly by the SIGNET Client Services Division (STC) and d
Canada and at missions abroad to all employees of the Department of Foreign Affairs and Intern

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