November 30

Computer Security Day 1995

Satnam Purewal
satnam.purewal@ubc.ca

Computer Security Day is November 30 and once again UBC is an official participant.

This year's theme is Management Support and I need your help. Please make all the members of your department aware of their security responsibilities on this day and throughout the year.

Everyone who uses a computer should take appropriate measures to protect their computer, computer programs and data. Every account is a possible entry point into a system. Choosing a good password reduces the risk of a security breach from your account.

History of Computer Security Day

Computer Security Day began in 1988 when the Washington D.C. chapter of the Association for Computing Machinery's Special Interest Group on Security, Audit and Control (ACM-SIGSAC) decided to bring extra attention to the issue of computer security.

> **take appropriate measures to protect your computer, computer programs and data**

The final business day in November was chosen for the annual Computer Security Day so that attention to computer security remains strong during the holiday season when it might otherwise become lax.

Participation is worldwide—from Korea to New Zealand to Argentina to North America. There are fifteen hundred organizations across the globe that will participate.

Good security practices

Depending on the type of computer you have and the systems to which you have access, your responsibilities vary. UNIX command-line access, such as that of a UNIXG account or Interchange Legacy, are much less secure than menu-based services such as Interchange Access and Express and Netinfo. If you do not need access to a UNIX command line, you should consider switching to one of the other Internet access services provided by University Computing Services. For more information about alternatives, please contact the Customer Support Centre at 822-2008 (e-mail **help@ucs.ubc.ca**).

Please consult the appropriate list(s) of security measures below for guidelines on how to ensure UBC's computer systems remain secure.

All systems

- Choose a good password (See "What is a secure password" on page 4 for details).
- Like your bank card's PIN number, *nobody* needs to know your account password. Do not share it with anyone.
- Review UBC's Appropriate Use of Information Technology policy. (You can view it on the World Wide Web at **http://www.ubc.ca/1/appropriate-use**)
- Check for computer viruses.
- Back up your data after being certain that it is virus-free.
- Managers: ensure that you have adequately trained secondary staff to manage your systems, in case your primary computing professionals are unavailable.
- Verify that passwords are not posted anywhere. If you must make a note of your password, then carry it in your wallet.
- Pay for and register all commercial software that is used on your computer.
- Pay for and register all shareware that you use regularly.
- Consider the privacy aspect of the data on your computer and protect it.
- Remember to log out after every session. Do not leave until you are sure your session has been terminated.

Computer security day 1995 *(cont.)*

All Interchange subscriptions

If you have an Interchange subscription, please add the following guidelines to your checklist:

- Change your password at least every three months. If it's been awhile since your last password change, do it today.
- Do not share your account or password with anyone.
- Check your file permissions. Ensure that all files are permitted appropriately.

Interchange Legacy subscriptions

If you have an Interchange Legacy subscription, please add the following guidelines to your checklist:

- Monitor your usage statistics. Do not wait until the end of the month or until you are out of funds to report the possibility of an unauthorized access.
- Avoid use of .rhost files.
- Avoid use of Internet Relay Chat (IRC).
- Review your .history file. Were all those commands issued by you?

SIS, FRS, IHRIS, Alumni

If you access the Student Information System, the Financial Records System, the Integrated Human Resource Information System (IHRIS) or the Alumni system:

- Notify the appropriate person if you will not be using your account for more than four weeks. Your account should be suspended while you are away.
- If you are logged in, please log out before leaving your work area.
- If you use the secure call-back system, do not share the dial-in number.
- All information viewed on these systems should be treated in a confidential manner. Don't let anyone look at your screen.
- Review last login data. Was it you? (Last access data is displayed during the login process).
- Review the number of invalid attempts since you last signed on. Is someone trying to guess your password?

Report any problems

If you notice any strange activity or files on your computer, or if you think that your account may have been compromised, please report it immediately to Satnam Purewal at 822-4820 (e-mail **satnam.purewal@ubc.ca**).❑

Satnam Purewal is a security analyst, Administrative Technical Support, University Computing Services, Computing and Communications.

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