

November 30, 1994

Participate in computer security day

Satnam Purewal

satnam.purewal@ubc.ca

This year's international computer security day is Wednesday, November 30.

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

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

You participate in computer security day where you live and work, not at a remote conference or meeting. This year, more than one thousand organizations around the world will participate. UBC is one of them.

The theme this year is *individual responsibility*. Everyone who uses a computer should take appropriate measures to protect their computer, computer programs, and data.

If you already take steps to ensure that your computer systems are secure, congratulations. If not, mark November 30 on your calendar as the day you begin your new computer security practices.

We ask that all UBC employees and students participate in computer

Fourteen steps to computer security

Good computer security requires more than a good password. This list outlines all the things that constitute good computer security practice. Most or all of them should be performed by anyone who has a computer at their home or office, to ensure a secure and problem-free computing environment.

1. Change your password if it has been more than three months since you set it.
2. Check for computer viruses.
3. Back up your data.
4. Delete unneeded files.
5. Place write-protect tabs on all diskettes that are not to be written to.
6. Verify your inventory of computer applications.
7. Verify your inventory of computer utilities and packaged software.
8. Verify your inventory of computer hardware.
9. Register and pay for all commercial software that is used on your computer.
10. Register and pay for all shareware that you use regularly.
11. Install and inspect power surge protection as appropriate.
12. Install fire/smoke detection and suppression equipment in computer areas.
13. Verify that passwords are not posted and that computers are physically secured.
14. Verify that all source code is protected from unauthorized changes.

security day on November 30 by doing at least one of the suggested security checks outlined in the sidebar. □

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