Create a special Download directory/folder. Put all downloads into this special directory/folder. This helps to keep malicious software from your valuable data.

In your Mail Client ***never*** allow remote website graphics. Choose the option that reads something like this - block loading of remote images in mail messages. Do not allow java or javascript. Beware of attachments. Never open an attachment unless you are expecting it. If it is unexpected from a friend, child, parent, it could be spoofed. If it's from someone you never heard of, delete that email.

Another strategy is to have two email addresses. One is a private email which you give out to people you want to contact you and no one else . Get a public email address, using Yahoo, Netscape, etc. Use this email address to log onto public sites. Treat any email sent to this account as suspect.

A word about wireless

Are you using wireless? Have you set a password? It is not illegal for someone else to hijack your wireless connection. Here's a true story: A friend and I were riding elevators in a high rise filled with law offices. We discovered that most of the law offices had wide open wireless connections for anyone to steal their data using a wireless connection. So, do not leave your wireless port open all the time to allow any stranger entrance into your machine.

Use partitions

Here's a proactive option that can be better than depending on expensive reactive anti-virus software that's often hard to keep up to date. Either split, or partition, your hard drive into two sections or get a second hard drive. To partition you will need to use partitioning software such as Paragon Partition or Partition Magic.

One hard drive (partition) contains your personal data and never ever sees the Internet. Do not name this C: drive. Viruses and worms hunt for the C: drive, and so does spyware lurking in RAM. It may be best and easiest to get an external hard drive which will be identified as D: for your secure partition. For Unix, Linux, and BSD, set the home directory permissions on the personal data drive to 700. Consider setting up your machines with internal and external nets.

The hard drive (partition) used to browse the World Wide Web and for email has no personal information on it, including email address books. Use a flat text file, if you must have an address book Many viruses and worms are written to go after address books.

Remember*!* Unplug your Internet connection when reading or doing any work on your secure private drive. Just like pregnancy, it only takes *one* unprotected moment.

Some people believe that some of these horrific viruses and worms that shut down entire hospitals, businesses, universities, research centers are being used to create SPAM search engines. At least, the Internet hard drive should be wiped monthly. Loading Linux on this drive will provide an added layer of protection. Finally, do backups of your email.

Here's a true story about Linux security: A friend was trying to do a purchase over the Internet with a company, but she had no success. Finally the company's rep said, "You are using Linux. We can't read your hard drive. We can read Windows and MACs not using OSX." So, just by doing an Internet purchase, you could be opening the door to your hard drive and the confidential information on it

A final word of advice: If you have an employee who downloads something into your untouched-by-the-Internet hard drive (partition), fire that person. Would you tolerate an employee who left your office doors wide open after hours?

Hopefully, following the above security ideas will keep you, your family and your company safe from pirates as you sail the Internet seas.

About the authors: Alexandra Andrews is a Linux Webmaster for about 15 sites, including CancerLynx.com, CancerSupportiveCare.com, TheCancerAnswer.org and Self-Sufficiency.org. Neil Dunlop is chair of the Computer Information Systems Department at Vista Community College in Berkeley.