Here are additional thoughts on concocting passwords from your favorite book:

- If the words end up being the same, pick another word. And pick different words if the combination seems too commonplace, such as WestWind or FootBall.
- For an interesting variation, insert a couple of numerals or special characters between the words. You end up with passwords like into#cat, ball3%and, or tree47wing. If you want, use the page number of the second word as a separator. For example, if the words are *know* and *click* and the second word comes from page 435, use know435click.
- To further confuse your friends and enemies, use medieval passwords by picking words from Chaucer's *Canterbury Tales.* Chaucer is a great source for passwords because he lived before the days of word processors with spell-checkers. He wrote *seyd* instead of *said, gret* instead of *great, welk* instead of *walked, litel* instead of *little.* And he used lots of seven-letter and eight-letter words suitable for passwords, such as *glotenye* (gluttony), *benygne* (benign), and *opynyoun* (opinion). And he got A's in English.


TIP

- If you use any of these password schemes and someone breaks into your network, don't blame me. You're the one who's too lazy to memorize D#Sc$h4@bb3xaz5.
- If you do decide to go with passwords, such as KdI22UR3xdkL, you can find random password generators on the Internet. Just go to a search engine, such as Google, and search for Password Generator. You'll find web pages that generate random passwords based on criteria that you specify, such as how long the password should be, whether it should include letters, numbers, punctuation, uppercase and lowercase letters, and so on.


TIP

Recent research is suggesting that much of what we've believed about password security for the last 30 or so years may actually be counterproductive. Why? Two reasons:

- The requirement to change passwords frequently and making them too complicated to memorize simply encourages users to write their passwords down, which makes them easy to steal.
- A common way that passwords are compromised is by theft of the encrypted form of the password database, which can then be attacked using simple dictionary methods. Even the most complex passwords can be cracked using a dictionary attack if the password is relatively short; the most important factor in making passwords difficult to crack is not complexity but length.