You can slow down a hacker by using names that are more obscure. Here are some suggestions on how to do that:

- Add a random three-digit number to the end of the name. For example: BarnyM320 or baMiller977.
- Throw a number or two into the middle of the name. For example: Bar6nyM or ba9Miller2.
- Make sure that usernames are different from email addresses. For example, if a user's email address is `baMiller@Mydomain.com`, do *not* use baMiller as the user's account name. Use a more obscure name.

WARNING

Do *not* rely on obfuscation to keep people out of your network! Security by obfuscation doesn't work. A resourceful hacker can discover the most obscure names. Obfuscation can *slow* intruders, not stop them. If you slow intruders down, you're more likely to discover them before they crack your network.

Using passwords wisely

One of the most important aspects of network security is the use of passwords.

REMEMBER

Usernames aren't usually considered *secret.* Even if you use obscure names, even casual hackers will eventually figure them out.

Passwords, on the other hand, are top secret. Your network password is the one thing that keeps an impostor from logging on to the network by using your username and therefore receiving the same access rights that you ordinarily have. *Guard your password with your life.*

Here are some tips for creating good passwords:

- Don't use obvious passwords, such as your last name, your kid's name, or your dog's name.
- Don't pick passwords based on your hobbies. A friend of mine is a boater, and his password is the name of his boat. Anyone who knows him can quickly guess his password. Five lashes for naming your password after your boat.
- Store your password in your head — not on paper.

  WARNING

  Especially bad: Writing your password down on a sticky note and sticking it on your computer's monitor.