The South Bay Mug

MACINTOSH

A Monthly Cupful For South Bay Apple Mac User Group Members, Jan. 2007

MACHinations

A personal view from Bob

Who's There?

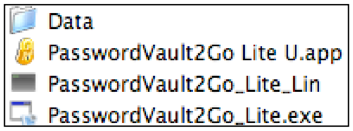
Just as you lock your house and car, you should use passwords to protect your Mac and it's contents. There are bad guys who will take advantage of any open door. In OS 9 passwords were optional; in OS X, they are de facto. You may complain about having to enter a password to install software or make changes to the System, but it's to protect you. Years ago you only worried about someone with physical access to your Mac; now with full time connections to the Internet, a hacker anywhere in the world is a potential thief.

How much security do you need? Assess your risk. Are you a casual Mac user with little of value or do you use it for business and finance? Apple assumes you're the former and auto-login is enabled by default. Apple's Keychain, where many of your passwords are stored, uses your login password and is automatically unlocked when you log in. If someone, who may do you harm, has physical access to your Mac, change your keychain password, and lock Keychain before going to lunch. This adds a level of security but is an additional hassle. That's life.

Out of the box a wireless router (base station) has encryption turned off and it's up to you to turn it on. Otherwise, with a blank or easily-guessed system password, someone parked in front of your house can access your hard drive, read and copy your files. Turn on WPA or WEP encryption on your wireless router. WEP is OK but WPA is more secure.

Password Managers. It's OK to use a simple password for benign stuff, but if serious money is involved don't use your pet's name or zip code. The more obscure, the better. Ed552C%^"Bn is a strong password, but how do you remember it? Keychain, Apple's built-in password manager, is automatically invoked for many activities, like accessing your mail, but for other things, like logging into a banking site, keychain doesn't work. Use a password manager. It's a database for storing passwords, user names and URLs. They range from free to $30. The password manager is locked with a master password that you should memorize. Many accept a pass-phrase, a long sequence like "SBAMUGmeetseverylastWedsinRB" that's easy to remember but hard to crack. Most store a URL that can automatically open the sign-in web page. Click-paste your user name and password into the login boxes.

PasswordVault and PasswordVault2Go cost $15. The Lite version is free but holds only 15 entries. There's a versions for the desktop and "2Go" versions for Mac (.app), Linux (Lin) and PC (.exe), that go on a flash drive. All use the same data folder, can be synchronized to the desktop application and opened on "any" computer so long as the flash drive has a universal format (Fat32), the default format.



Data
PasswordVault2Go Lite U.app
PasswordVault2Go_Lite_Lin
PasswordVault2Go_Lite.exe

Encrypted Disk Image. My August 2006 article described how to secure private files by putting them into an encrypted disk image. Don't open the disk image with keychain, unless you have a strong, separate keychain password and guard it carefully. Otherwise, if it's automatically opened when you turn on your Mac, your private files are available to anyone with access to your Mac.

Backup. Finally, be sure to back up your keychain files, stored in the System and user libraries, as well as password files and any encrypted disk images.

SBAMUG

Bob Brooks
Helping Beginners
310-545-8060
SBAMUG@gmail.com