Tips on Using KeePass

Information Technology Services
Iowa State University

December 13, 2007

KeePass is a small portable application that can store many username/password values. One “master key” is typically used to unlock all the stored values. The values are encrypted in a secure fashion so that if you don’t know the “master key” you cannot decrypt the database and retrieve the stored passwords.

Using KeePass is much more secure that choosing short/simple passwords, using the same password for everything, or writing down passwords on paper or insecure “computer notes”. Since passwords should be “long and complex” in today’s world of online “password crackers” and other evil-doers, keeping your set of complex passwords in a “password storage application” is a very good idea.

A few tips will help you get the most benefit from KeePass.

Tip 1 – Make sure all your passwords are long and complex

Think of a “password” as a “pass phrase”. Most modern security systems will allow very long passwords with spaces in them. A good recommendation is to make sure your “pass phrase” is 5-6 words, not a common phrase or slogan, contains upper/lower-case and punctuation, and has one misspelled word. An example might be “Kermit the Frog is knot yellow?”

Tip 2 – Make the master “Composite Key” a good “pass phrase”

Keeping all your complex passwords under a simple one provides no security. Use the rules in “Tip 1” to construct a secure “pass phrase”. Make sure the “password grader” (the colored bar below the “Composite Master Key” entry area) on KeePass agrees it is a secure pass phrase as you enter it.

Tip 3 – Don’t forget the Master Key!

KeePass IS secure. If you forget the Master Key pass phrase, you will have lost access to all your stored passwords. Tools are NOT available to recover a lost master password or any of the contained passwords.

Tip 4 – Backup the KeePass components

Backup your KeePass program and database on a regular basis. The database files are those with a “.kdb” (“KeePass database”) extension. Keep the backups in a secure place (so you know where to find them).

Tip 5 – Put KeePass on a USB drive

Putting all your passwords on your work computer will not help you if you need a password at home that evening for online shopping. Keeping two copies of KeePass (one at home, one at work) will make keeping them “in sync” frustrating as you change passwords. Get a small “USB drive” and place all KeePass components (especially the “KeePass.exe”, “KeePass.ini”, and “.kdb” files) in a folder called “KeePass”. Keep this USB drive with you, and use it on any Windows system (at home, at work, or “on the road”). Make SURE you use “Tip 4” and keep a backup the “KeePass folder” in case you lose the USB drive or it becomes damaged.