Tools for managing multiple passwords

Passwords should not be stored in cleartext

Local

- **1Password** – https://agilebits.com/onepassword
- **IronKey** – https://www.ironkey.com/news/verisign-ironkey-otp-password-service
- **KeyPass** – http://keepass.info/
- **PasswordSafe** – http://passwordsafe.sourceforge.net/

-

Hosted

- **LastPass** – Best used with two-factor authentication, such as **YubiKey**, **Google Authenticator**, or other option (**http://twofactorauth.org/**)
- Note: There always a possibility of a breach of the vendor

-

Password managers heavily rely upon a long and strong master password. One suggestion is to use an algorithm to create unique passwords based upon the site name or some other criteria. A tactic to consider is the use of a *pass phrase* versus *password*, as such emphasizes the length. Some good examples can be found at:

- http://www.dc214.org/notes/july2005/Mnemonic-Password-Algorithms.pdf
- http://www.seas.ucla.edu/security/passwords.html

Revision #3
Created Fri, Jul 8, 2011 2:07 AM by MacKnight, Scott
Updated Sun, Jan 11, 2015 11:23 PM by Postovoit, Philip