

PASSWORD PROTECT YOUR MOST IMPORTANT DATA

A Sun City Summerlin Computer Club Seminar
Presented by Bill Wilkinson
January 2008

Your computer can be attacked by anybody. There is absolutely no privacy on most PC machines. Why? Because to get full functionality from your computer, you have no choice but to connect your machine to the rest of the world via the Internet. There is almost no machine in the world that is not connected. With such connectivity comes total vulnerability. A computer security guru who was interviewed on National Public Radio in February 2006, estimated that up to seven per cent of all the computers in the world have been hacked and are sending vital data (social security numbers, credit card numbers, passwords, etc.) back to the bad guys, most of whom are beyond the jurisdiction of the United States government and its laws.

Hacking (or cracking) no longer requires experts. There are thousands of off-the-shelf programs available on the Internet that are as easy to use as the software packages with which most of us are familiar. (Enter "hacking software" into the Google search engine and you will get 4,280,000 hits!) Anyone can use these packages to hack into your system. Unfortunately, there is no defined, requisite learning curve - the amount of knowledge or background essential to be an "effective hacker" is virtually zero.

Encryption (defined: to convert computer data and messages to something incomprehensible by means of a password key, so that it can be reconverted only by an authorized recipient holding the matching *password* key) is the only way to protect your important data. Encryption renders your data, even if accessed by an unauthorized person, unintelligible and unusable. By adopting the simplest prevention techniques, you can ensure complete data privacy.

The First Step is to Make A Good Password?

There are three major factors: **randomness, complexity, and length.**

Randomness. A good password will be a truly unique combination of characters, and that means that the password should not appear in any form in any dictionary (in any language), book of quotations, and so on. The password also should not be based on simple substitutions or transpositions of common words or phrases: If any underlying pattern remains it becomes easy to crack.

Complexity. For example, if you limit yourself to the lower-case letters of the English alphabet, each character in your password will have only 26 possible values. Simply allowing uppercase and lowercase letters means that each character in the password can have 52 different values. Add in numbers (0-9) and you have 62 possible values; add the punctuation and symbol characters commonly found on a US-English computer keyboard, and you have a total of about 92 unique (non-repeating) possible

values. Clearly, using all the kinds of characters available to you significantly increases the complexity of a password.

Length. A two-character password, where each character could be any of 92 possible values, affords just 8464 (92X92) unique combinations. Three characters allow 778,688 (92X92X92) possibilities; four yields 71,639,296 (92X92X92x92), and so on. So clearly, longer passwords are better because the number of possible character combinations increases exponentially with length.

Online Calculator Will Estimate the “Cracking Time” for Various Passwords

While something like 71,639,296 password possibilities would be daunting in human terms, it's nothing to the brute strength of a PC with “cracker” software installed. An online calculator (located at <http://tinyurl.com/mqes6>) lets you play with variables to see how long a "brute force" password-cracking program would have to run to defeat passwords of varying lengths and complexities. Note that the "speed -- thousands of passwords per second" figure depends not only on the speed of a given PC, but also on the efficiency of the cracking software, which is a huge variable in itself. But the calculator is seeded with an exceedingly low number, which significantly under-represents the power of today's PC's and software. For a more realistic view of contemporary threat levels, crank up the "speed" variable by several orders of magnitude. (For a hardware-based starting point, you may wish to note that the common Intel Pentium processor is capable of processing hundreds of millions of instructions per second.)

Create strong passwords that you can remember

You could come up with a completely random combination of numbers and symbols for your secure password, but that's not very practical. How would you remember it? Chances are you'd write it down and keep it in the top drawer of your desk and then it's no longer such a great password after all, particularly if it is lost or misplaced.

A strong password is one that is at least eight characters, includes a combination of letters, numbers, and symbols and is easy for you to remember, but difficult for others to guess.

Create a strong “passphrase”

The easiest way to create a strong password that you won't have to write down is to come up with a passphrase. A passphrase is a sentence that you can remember, like "My son Jeff is two years older than my other son Brant." You can make a pretty strong password by using the first letter of each word of the sentence. For example, msjityotmosb. However, you can make this password even stronger by using a combination of upper and lowercase letters, numbers, and special characters that look

like letters. For example, using the same memorable sentence and a few tricks, your password is now M\$Ji2y0+^^0\$B.

If you think that a phrase that you have made up is too hard to remember, you could try a more common phrase, such as "You can't teach an old dog new tricks." If you're using a common phrase make sure to inject at least one number or symbol into the password. Such as "U(+@0dn+”.

Other examples of passphrases (passwords)

4\$@7y@rfbfo+(translation: “Four score and 7 years ago our fathers brought forth on this continent...” (13 “random” characters)

yd7n40@dwwlii translation: “Yesterday, December 7, 1941 - a date which will live in infamy” (13 “random” characters)

@nvvy((d4y@vvu(d4y(translation: “Ask not what your country can do for you, ask what you can do for your country.” (19 “random” characters)

The Cypherix Program: an encrypted vault for your private data

This is where a free security program, **Cypherix**, comes in. The Cryptainer encrypts and protects data that is created on your PC. It allows you to create an encrypted "vault" where you can store all data of any kind, e.g., personal finance records, income tax data, banking records, stock market portfolios, important email messages, and important word processing documents, to name just a few. **This simple, easy to use encryption software creates an encrypted virtual drive, provides password protection and hides any file or folder ensuring file encryption, automatically.** Its powerful encryption (128 bit) ensures that only you can access your data.

$2^{128} = 340,282,366,920,938,463,463,374,607,431,768,211,456$ possibilities.

Cryptainer creates a separate volume (disk drive partition) on your hard drive that can only be accessed with a password. This volume stores files in the encrypted form. Once loaded via the password, the Cryptainer drive is like any other drive with which you normally work. By using Windows Explorer as your file management system, you can just drag and drop any file into the Cryptainer Vault. It is automatically encrypted. It's that simple! Cryptainer vaults can only be viewed, accessed, browsed or modified by the user who has the key (password) to open it. At other times, the “vault” or drive and all the files held within are absolutely invisible!

The “vault” can be transported (moved/copied) to any location (another folder, another drive or even to a CD). Cryptainer combines ease of use with state-of-the-art technology to ensure total security, zero learning curve and maximum convenience!

Cryptainer offers true on-the-fly disk encryption, making sure that absolutely anyone can use it effectively! What you get is foolproof, hassle-free, unbreakable computer security.

Follow these steps to download and install Cypherex:

1. Access the Internet via your favorite browser.
2. On the address bar, type this URL: <http://tinyurl.com/bkmhf>
3. Click on the blue and bright yellow **Download** button.
4. At the file download dialog box, click **Save**.
5. Save the application to your **Desktop**.
6. Close any Web Windows that remain open.
7. Double-click on the **cryle.exe** icon to start the installation wizard.
8. Click **Run**.
9. Click **Next**.
10. Click on the bullet next to "I accept the agreement"; then click **Next**.
11. Accept the default for the destination location by clicking **Next**.
12. Accept the default for the start menu folder by clicking **Next**.
13. Click **Install**.
14. Click **Finish**.
15. Delete the installation program file (**cryle.exe**) from the desktop.

Follow these steps to run Cypherex:

1. Double-click on the **Cryptainer LE** icon (a yellow triangle) on your desktop, or select it from the Start Menu.
2. If you are starting **Cryptainer** for the first time, you will be asked to specify certain details:
 - a. On the dialogue box titled **Specify Cryptainer Volume Details**, you will see a text box where you may specify the location and name of your volume file. Use the **Browse** button to choose a location of your choosing (suggestion: My Documents), as well as a file name for the Cryptainer Volume (suggestion: **Encrypted Data**).
 - b. Accept the default, Cryptainer, for the volume label.
 - c. Increase the file size that you want allocated for the Cryptainer volume file to the maximum of 25 MB. (Recommendation: try the free program that has a maximum capacity of only 25 MB. If the program suits your privacy and security needs, then consider upgrading to a Cryptainer that has more storage capacity.)

- d. Enter a password that will be used to load the volume file as a Cryptainer drive. **HERE IS WHERE YOU WILL WANT TO ENTER A STRONG PASSWORD! THIS ISSUE WILL BE DISCUSSED IN DETAIL.**

IMPORTANT CAUTION!!!!!!: If you forget your password you cannot access the Cryptainer volume. There is no special procedure, secret code, or hidden entry method to fall back on.

- e. Re-enter the password in the Verify Password box. Do not use "Paste". You must type the password again so as to avoid any inadvertent typing errors.
 - f. Click on the button **Proceed to Create Volume**.
 - g. If you get an error message at this point, you must remove the compression attribute for the Encrypted Data file that you added to your My Documents folder. We will demonstrate how to eliminate the error during the seminar.
 - h. The Cryptainer volume file is then created. After the creation is complete, this Cryptainer volume file is then loaded as a new drive.
3. On subsequent starts, Cryptainer asks you for the password to load the volume. Enter the password, and click OK.
 4. Note the letter (usually D) that has been assigned to the new virtual drive.
 5. Open Windows Explorer and realize that Removable Drive D is a virtual (imaginary; non physical) drive that will contain all the files that you have stored (or will store) in your secure encrypted vault.
 6. You can move folders and files in and out of the Vault by using Windows Explorer's drag and drop method, copy and paste method, or edit method from the Menu bar. (These common editing procedures will be demonstrated at this seminar session.)
 7. When the encrypted files are "loaded", the Cryptainer drive will appear in Windows Explorer as a special hard drive volume (generally "D"). All the applications on your system can now use the encrypted files in your Cryptainer drive like any other files on your computer. The encryption and decryption processes occur transparently in the background.
 8. When you no longer need access to your encrypted files, it is important that you select either **Unload** the drive or **Shut Down Cryptainer**. This protects your encrypted information by removing/hiding the Cryptainer drive containing your files. Now, no one can access them without the password. (Note that the Cryptainer drive is now invisible in Windows Explorer.)

TIP: If you minimize or close your Cryptainer window by using the Resizing Tools in the upper right corner of the window, it is hidden. However, any loaded (open) volume still remains loaded (unlocked). You can always see this Cryptainer window by double-clicking on its icon that appears on your taskbar or systray (notification area).