

## CREATING A PERSONAL PASSWORD ALGORITHM

[January 2006]

© Victoria L. Herring, ([www.herringlaw.com](http://www.herringlaw.com))

### **Digits, digits, digits....they're taking over my brain and yours no doubt!!!**

As I recently wrote to David Rowell, creator of *TheTravelInsider.com* to discuss and explain about problems with some applications for password [user ID and password] generation or use:

"I was reading the article in this week's *TravelInsider* newsletter and it provided helpful information. I gather the product linked to is for Windows machines, but there are other products for Macs as well [there is also a built in password generation and testing program in OS X's Keychain Access, as part of the operating system]. The issue is of crucial importance as we stock our brain cells with all sorts of data and push out really useful information <grin>: not only do you need a password, you need to know the URL, you need the user id that is associated with the account and you need the password.

One problem with the application written about in *TravelInsider* and with others is that it is apparently machine-specific. It appears to be associated with a certain browser's use on a certain machine. However, for various reasons people are using more browsers interchangeably thus requiring redundancy of installation. Therefore, it is less portable and useful unless it is used with one's laptop, only, or the information is easily synchronized and transported to others. However, I did not do a lengthy review of the program and perhaps that browser-specificity is not so limiting.

I use [for my Mac] the program Password Wallet by Selznick Scientific Software ([www.Selznick.com](http://www.Selznick.com)) which is shareware and there is a Palm version too so that you can sync the 'wallet' of data with your Palm and it is transportable in that fashion.

Yet, one of the best password generation and use tools I've seen comes from a Podcast I happened upon one day for *Security Now* with Steve Gibson, which you can find at the iTunes Music Store [available for both Macs and Windows] and in text version at GRC's "Security Now!" [Episode 4, Personal Password Policy] ([www.grc.com/securitynow.htm](http://www.grc.com/securitynow.htm)). Basically, what the Podcast advocates is to come up with an algorithm of your own that you can apply on a per-site basis. In other words, rather than use a static password that can be easily guessed or hacked, you use one which changes with each website visited but is fairly secure in itself. [I'll explain below with a totally made-up example which others should not now use]

For instance, you have a password-type set of letters and digits to which you apply something unique about the website name, and you have a personal password that is specific to that site but relatively easy to remember. Let's say you decide that you will

*Creating a Personal Password Algorithm, page 1*

© Victoria L. Herring, ([www.herringlaw.com](http://www.herringlaw.com))

use the 3rd and 2nd letters of the website name coupled with some other odd mix of letters/digits that you can and will easily recall because you'll use them all the time. If we use the example of the following and apply it to each website, you can see how it morphs depending on who is sitting there at the computer, regardless of the location, regardless of the browser, regardless of whether it's Windows or Mac or Linux or other and it changes with each website with a minimal need to remember the entire password:

**X2T4vw** [let's say for instance that is your memorized code. A gibberish mixture of caps and regular letters with numbers].

Your personal code that associates with each website without variation is that you take the website name and use the 'first' two letters in caps and follow then with one, two or three more digits. So, if you pick "357" as your ending digits you would have passwords for websites that would vary with those sites but be fairly easy to remember, but hard to guess:

CNN: X2T4vw + CN + 357 = X2T4vwCN357

Washington Post: X2T4vw + WA + 357 = X2T4vwWA357

LovelySmurfs.com [fake site name]: X2T4vw + LO + 357 =  
X2T4vwLO357

Of course, if there is a keystroke recorder on machines [as might happen away from the office or home] you might need to change passwords the next time you go online to a site [which is a pain, of course] but that may be fairly rare and it might be fairly easy done because that time you just change the code you are using. Perhaps you keep everything but switch the order, start with 357 and then follow with the 2 or 3 letters and then with your secret weird digitizing.

This may be something to use mainly with high-security sites and not with simple read-only sites, such as when you want to 'register' for a newspaper or to access a forum but where no personal data is stored. In that case, memorize something unique [again, a mix of digits and letters, not one word or two] and just use that. So, you'd have one password that is extremely secure and another which is a throw-away password, where you don't care whether people also access the site.

And then you could also realize that life's too short to spend time with this and you don't much care if anyone has your personal data, but then you'd be wrong."

I hope this helps. As I was traveling recently, it was amazing how easy it was to remember and put in the right password each time!