So many passwords, so little memory

April 15 2009, By Craig Crossman

How many keys are on your keychain? I just looked at mine and counted nine keys. And that's not counting the bulky little remote control key fob that locks and unlocks my car. I've tried to consolidate my keys by making one key fit every lock in the house instead of having different keys for the front door, the back entrance, the shed and some of the different rooms that lock. Then I thought about making just one key that would work for everything.

One key to lock the house, unlock the car, open the Post Office box, access the storage unit I rent, get into my bank's storage box, open the office door, you get the idea. And while that idea would certainly reduce the number of keys I have to lug around with me every day, having just one key for everything would actually be a bad idea, especially when it comes to the issue of security.

Think about it for a moment. What would happen if I lost my one key or even worse, somebody stole it? If I just had nine or 10 different locks, it wouldn't be too bad. I'd just have to change all the locks or at the very least have all of them re-keyed. But what if I had 100 locks or more? That could be a real problem. Yet when it comes to passwords, this is exactly what a lot of us do. Because we have so many passwords guarding all those websites we access and programs we use, it's become a real problem trying to create and then remember so many different passwords for all of them. Yet this is what is being demanded from us when we go someplace online for the first time and that place is designed to store something relevant to us so we can revisit it repeatedly. You need a password to secure it. And that's not even counting all of

your applications that require a level of security such as your checkbook program.

Believe it or not, there's a lot of people out there using just one password for everything and they do it because basically they just can't remember a unique password for all the places they go and products they use. Yet having one password for everything is like having one key. It's a bad idea. Losing or forgetting a password is far easier to do than losing a physical key. It's a lot more common than you may think. People forget passwords every day. Just take a look at most websites that ask for your password. Most all of them have a question that asks if you've forgotten it! Typically they will either e-mail it to the address you registered when you first applied for the password or they will let you pick a new one once your identity has been verified. Still it can be a big mess. Fortunately, there are utilities out there that are designed to manage all of your passwords so you won't have to remember any of them.

If you have Windows PC, check out Password Manager ($29.95) from Large Software. If you have a Macintosh, check out 1Password ($39.95) from Agile Solutions. Password Manager and 1Password will remember all of your usernames (you can forget those too) and passwords for every website you visit and the applications you use. Both utilities will work with most any of the popular browsers such as Firefox, Internet Explorer, Safari and Opera. They will even import all of your existing passwords stored in the browser and deactivate the browser's password feature. All of your password information is heavily encrypted by these utilities yet no bridges are burned. If you later decide not to use them, the password file used by your browser will be restored.

Another nice feature offered by these utilities includes being protected from phishing scams that pretend to be legitimate websites so that they might trick you into entering your passwords. Password Manager and 1Password both have smart form fillers that can recognize phishing sites

and will not release your password information to them.

When you are away from your computer, both utilities offer a memory stick ability that lets you take all of your passwords with you. When using another computer, simply insert the memory stick into any available USB port and that computer's browser will know to fill in your usernames and passwords whenever you access a website to which you have an account. Removing the memory stick takes all of your password information along with it and nothing remains on the borrowed computer.

Passwords are the virtual keys of our time and they need the same, if not even greater protection than your physical keys. Never write your passwords down nor store them in a word processing document where they may be easily discovered. And don't use obvious passwords like your name or birthday. Passwords really should not be words at all. They should be a cryptic combination of letters, numbers and if allowed, punctuation marks. Given the complexity and the large number of passwords we require these days, a password manager really is the best possible solution to a cryptic problem.

On the web:

Password Manager: www.largesoftware.com

1Password: www.agilewebsolutions.com

(Craig Crossman is a national newspaper columnist writing about computers and technology.)

___