Tech Coach Corner – Password Manager? We Don't Need No Stinking Password Manager (Part 1)

by LTCL Tech Coach Jeff Lazar

You've heard about them, you've read about them, and if you've come into the library for some in-person tech support, you've probably experienced one of the coaches asking you if you use one. But if you are still using your wedding anniversary or your child's birthdate as your universal password, it's only a matter of time before you will regret it. When companies such as Adobe, Marriott, eBay, LinkedIn, and Yahoo have experienced major security breaches, the need for a password manager has never been greater. About 3.5 billion people saw their personal data stolen in the top two of 14 biggest breaches of this century alone. The smallest incident on this list involved the data of a mere 134 million people. While I won't make specific recommendations about using a particular password manager (PM from now on), I'll offer some things you need to consider in Part 2 coming in a week or so.

What exactly is a password manager?

The short answer is to think of it as an electronic replacement for those scraps of paper, Post-it notes, and notebooks that you use to keep track of all your passwords. Come on now…you know you do this. So, admit it's a bad practice (what happens if you lose that little notebook?) and look at the benefits of a PM.

Using a PM means you will need to remember only one password – the master password for the PM itself. Many of the PMs will ask you for it every time you attempt to use it; others have a setting that you can tweak. For example, mine has a default of forcing me to enter it every 30 days even if I tell it not to ask for it – it's a small price to pay for peace of mind.

Most of the better PMs will "grade" your password for you – you always want a strong one that mixes upper- and lower-case letters, numbers, and symbols. The better PMs will actually generate a password for you! Here's one that my PM just generated for this article: c%@ryC77j7pA#J3Q. Try and hack/guess that! It's super strong, and I don't have to remember it.

Most of the PMs will work across platforms – I have an iPhone and an iPad, but my work demands that I live in the Windows world (with both a desktop and a laptop). My PM predates my wandering into the iOS (Apple) world, but it works well in both worlds.

Is a PM a magic pill? Not quite. You might need to change all your passwords, once your PM calls them all weak. You might need to pay for a PM (although there are a few good ones available at little or no cost). You will need to learn a new piece of software – but most have very user-friendly interfaces. You'll still need to remember to change your passwords frequently. (I change my key ones – bank accounts, brokerage accounts, etc. monthly.) You'll still need to use two-factor authentication (conventional password plus a code that is either emailed or texted to you with same important places just mentioned). And don't forget that your mobile phone and tablet need to have their screen locks set! We see lots of folks who don't do this – especially with their phones. Finally, use only computers that you know and trust -- in other words, don't use an "open" computer for anything that is secure and normally requires a password. This includes airports, Starbucks, and even our library. And never, never, never reuse a password; that's the hidden beauty of a good PM.

What will it cost? There are free PMs as well as others that you can expect to pay roughly $50 per year, with multi-year discounts generally available. I'll review different PMs in Part 2 of this column (stay tuned).

Other Decisions?

Before we get to programs and costs, there is one more decision to face – Do you trust your passwords to be on the company's server ("in the cloud"), or do you want total control (meaning keeping them on your device locally)? You do have options with some of the PM. I allow mine to be stored in the cloud – it just makes my life easier and doesn't matter which device I grab. In addition, my passwords are encrypted end-to-end, which offers another layer of protection. The decision to keep your passwords totally under local control means it is absolutely essential that you have a daily backup routine…you simply cannot compromise because the risk of losing your passwords is too great. With cloud storage, your passwords are always available to you, even if all your devices crash or are lost.

Stay tuned for Part 2 on this important topic!