smallbiz
technology
Tech insight and news for small business

Stop Remembering Passwords And Switch To Identity Management!

Posted on October 24, 2012 by Miguel Leiva-Gomez in Secure Your Data with 11 Comments

Chances are you’ve got a Facebook account, a Twitter account, a Google account (maybe even two), and several other accounts to cloud services you use all over the Web. Not only do you have to remember the URLs to these places, but you also have to remember every username, email, and password ever assigned to these accounts. Can you still do that when 2013 rolls in and you have to get into an account you last accessed back in 2010?

Do you even use different passwords? About a quarter of all Americans are estimated to use the same password for literally everything. A much larger amount use the same password for more than one account, perhaps limiting themselves to three “main” passwords. A few months ago, Yahoo fell victim to an attack in which almost half a million passwords were leaked. For those who use the same password for every service, that’s a really tough one to bite. Many accounts were accessed, and several people’s PayPal accounts froze because of illicit account access.

So, how do you manage to have more than 20 different passwords without going nuts? The answer: identity management, sometimes also referred to as password management.

With identity management, you create one single “identity” on the Web where all your passwords and usernames are stored. In other words, all of your passwords go into a secure database on a remote cloud server, allowing you to log in automatically to websites with a single click. The process is much simpler than you think.

Currently, there are two services offering automatic logins to websites through password management: SmartSignin and LastPass. I’ve had the pleasure of trying both services, so I’m going to compare the two.

All in all, both services do a decent job of encrypting your information, meaning that all of the passwords you put into their servers will remain encrypted and safe. The only problem is that you don’t have control over the encryption process when you use LastPass. SmartSignin does a really good job of letting you create your own encryption key to lock any data you put into it, even locking it from SmartSignin itself. They literally cannot see or make sense of anything you put in there because you’re the only person with the key that unlocks it.

In the user-friendliness department, SmartSignin wins again. LastPass has some really cool features, but they're very confusing and lead to a load of trouble for someone who's just looking for something with a smaller learning curve. If you want all the bells and whistles, though, LastPass is your best bet. If you want something you can just use right out of the box, go for SmartSignin.

LastPass and SmartSignin both have enterprise offerings, although it's a little harder to find the one for LastPass. If you want it, you can find it here. The pricing on both services is definitely attractive, but I highly suggest using SmartSignin for a full enterprise environment, as it has a more secure platform that's easier for your employees to learn.

Whatever service you choose, make sure it's right for you, your employees, and anyone else who's going to use it. Perhaps one of the best things about using identity management is that you get to save time while providing your business with a complete security blanket over your online "you."