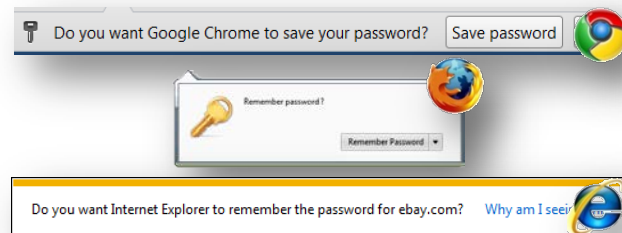


The Evils of Browser Password Remembering

Plugging a browser security hole while making access to your business applications more accessible

Do you let your browser store the passwords to your corporate web-based resources? Do your employees?

If you do, you should really re-think that strategy.



The Problem

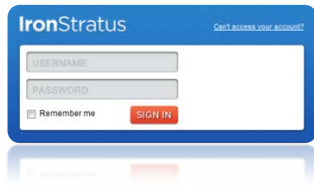
Browser “password storage” is really great, isn’t it? Not only is it convenient when you surf to a site, since you don’t have to type in the password, it also remembers all of those different passwords that you would probably forget otherwise. I use it for my personal passwords all of the time.

But what about for “business” passwords? If your business is like mine, more and more of your corporate assets and processes are finding their way into the Cloud. Our bank accounts, payroll, and sales database (among many others) are in the Cloud. What about the passwords for those sites? It may surprise you to learn that many businesses like ours are banning the storage of passwords in the browserⁱ. And it is for very good reasons (in priority order):

1. Passwords stored in the browser are tucked away on the hard drive of one particular computer, for one particular user. If that user or computer isn’t available, then neither is that password – potentially locking you out of a corporate resource. This can make normal events like vacations very problematic.
2. For most browsers, the passwords are stored in an insecure fashion on the hard-drive of the computer. This means that the person who just stole your laptop may have gotten more than just the hardware. But even if you’re not a laptop user, your obsolete discarded computer or failed hard-drive may still hold the passwords to your corporate Cloud accounts and can be easily discovered by someone nefariousⁱⁱ.
3. Browser password “remembering” doesn’t work for all sites – so you still have to write down passwords on sticky notes, or in a file on your hard drive. And anything you put on your hard drive is subject to problems #1 and #2.
4. Each browser stores passwords differently. So updating or even changing browsers becomes a big problem.
5. We aren’t all glued to our desk – needing to travel or even work from home. Browser-stored passwords can make this impossible for certain activitiesⁱⁱⁱ.

Essentially, the problem falls into one of business **Continuity**, **Security**, and **Accessibility**.

The Solution



The solution is IronStratus.

IronStratus is a cloud-based application that obviates the password storage function of the browser, but does it in a way that allows you to keep your business assets accessible and secure – eliminating all of the problems above.

Accessibility & Convenience

Since it is a Cloud application, you can reach IronStratus from anywhere you can connect to the Internet, and from any of the major browsers you are likely to use on your computer^{iv}. This means that you have access to your Cloud-based applications at work, at home, and on the road. Your passwords and login credentials aren't locked away in the browser on your desk-top machine at work. In fact, even if you use one browser at work and a different one at home, you have equal access to your login information from both places.

One of the nicest things about IronStratus is not only does it store your login information, it can also log you in to your applications with a single click. That's even more convenient than the password storage in your browser.

In essence, you get the convenience of browser password storage with the accessibility of an online application. Convenience with accessibility – the best of both worlds!

Continuity

Although convenience and accessibility are things you notice every day, it's the things that you don't see every day that may concern you even more. If you save your passwords in your local browser, you should ask yourself the question: "if my computer disk crashes, do I know the passwords for all of my applications?" Hopefully, you do a thorough backup of your desktop computer. Hopefully, too, the format of the backup login data is compatible with the new browser you choose. And hopefully you really don't need access to your applications for the hours necessary to get everything back up and running.

The issue here is business continuity. You need to keep your business running even when the inevitable disk crash occurs. IronStratus securely stores your Cloud logins and provides fulltime access to all of your Cloud-based applications. If one of your machines crashes, then simply go to another to access your critical applications. Even more critical failures such as fires or theft are mitigated through the use of IronStratus.

While disk or computer failures are unpredictable, they are also fortunately somewhat rare. One thing that isn't rare, however, is employee vacations and employee turn-over. And these two things are often the most frequent source of business discontinuity.

If one of your employees takes her normal two-week vacation in June, and all of her passwords are stored in the browser on her desktop computer, do you have enough access to keep the business running? But maybe more

importantly, if one of your employees leaves under less-than-wonderful circumstances, will he be cooperative in retrieving the login information from his desktop machine?

You can't afford to wonder about these questions. IronStratus stores all of your Cloud application login information making it fully accessible, independent of who is on vacation or who has left the company.

Security

But what about security? How secure are those passwords that are stored in your browser?

Modern browsers store passwords in an encrypted form using the password that you use to log in to your system (assuming you use one). And with a strong login password, these browser-stored passwords are relatively safe. That is, they are safe until a hacker gets ahold of your machine or the disk drive from it.

There numerous "password crackers" available for systems such as Microsoft Windows. When these programs are given unfettered access to a windows disk drive, they can "recover" or "crack" windows passwords in minutes, if not seconds. Then, once these programs discover your account password, the hacker can easily recover the passwords to all of your web sites stored in your browser.

More Information

There are numerous articles, blogs, and comments about the security of storing passwords in the browser; here are a few. For more information, trying doing a Google search for "are the passwords stored in my browser secure?" Or try "should I let the browser store my passwords?"

<http://msdn.microsoft.com/en-us/magazine/cc163958.aspx>

<http://www.howtogeek.com/68231/how-secure-are-your-saved-internet-explorer-passwords/>

<http://www.howtogeek.com/70146/how-secure-are-your-saved-chrome-browser-passwords/>

<http://www.symantec.com/connect/articles/password-management-concerns-ie-and-firefox-part-one>

Wrap-up

Just in case you missed it in the articles referenced above, here is a quote from the Microsoft article:

"Microsoft® Internet Explorer has built-in support for helping you remember passwords. So why is it that most companies (ironically, including Microsoft) encourage their employees to avoid this feature?"

Suffice it to say, for your business, using the browser to store your passwords is a bad decision. A good decision is using IronStratus. Surf to IronStratus to learn more.

For more IronStratus use cases, please check-out the IronStratus web site at www.ironstratus.com/what-we-do

ⁱ In this document my comments refer primarily to the Microsoft Internet Explorer®, Firefox®, and the Google Chrome™ browsers. There are others, and they all suffer from all or some of the problems highlighted here to differing degrees.

ⁱⁱ Some browsers are trying to solve this problem with “master passwords” which help a bit.

ⁱⁱⁱ Some browsers are trying to solve this problem by allowing the browser to “sync” passwords to the Cloud. If you ask me, this tells us that these browser companies realize that storing passwords locally is a problem.

^{iv} IronStratus works with Microsoft Internet Explorer®, Firefox®, and the Google Chrome™ family of browsers.