

Why Passwords are Worth Millions

Password security is no longer optional for businesses or individuals who are using cloud resources

Think your business is safe from mistakes by employees and cyber security attacks? Do you think all the security breachesⁱ you read about are because those companies are lazy or careless?

Passwords are quite literally the “keys” to all your business assets...every account, application, and protected website you use. Like it or not, passwords stored on your computer can be compromised, even if they are stored locally in an encrypted form. If someone can guess, capture or retrieve your passwords, you have just exposed your own identity, your private data, your company, and potentially all of your clients to that breach and potentially significantⁱⁱ (\$7.2-million per incident on average) financial or legal repercussions.

The Problem

Isn't it great that no one is looking over your shoulder and you can “cheat” on security by using your favorite strong password, or a slight variation, for password protected sites or business applications you register for? After all, your favorite password is strong and you've used it for years without a problem (as far as you know).

Here's a little test for you... which is the stronger passwordⁱⁱⁱ: “\$Fu&1d3!” or “D0g.....”? If you were a hacker and you wanted to crack the encrypted versions of these two passwords, you would rally a massive parallel attack from the Internet and generate about 100 trillion password guesses per second. The amazing thing is, using that approach; one of these passwords can be cracked in less than two hours, while the other one will take approximately 16,500 years.

Can you figure out which is which? Type them in at the GRC Haystack website to discover for yourself: <http://bit.ly/ykCsAy>. The point is, don't be too sure your passwords are safe. The ground rules for security (both personal and business) have changed dramatically over the past 2-years and the stakes are much higher now.

Now that cloud computing is the default way businesses run, you can no longer simply hope that you won't be a victim of a cyber-attack or a password breach. Everyday your risk goes up because the number of incidents is accelerating^{iv}; multiplied by the number of people you work with and for, so it's no longer a matter of if, but when.

The Solution

You need to have all your assets, securely accessed, managed and controlled in a single place and that place is IronStratus.

IronStratus is a cloud-based product that utilizes a specially designed browser add-on to ensure secure communication between your browser and the IronStratus server (all data transferred between your browser and the IronStratus server is protected with HTTPS and SSL). All decrypting of credentials in your vault are performed locally in the IronStratus browser add-on when you are logged into IronStratus. Your login password to IronStratus is the encryption/decryption key to all vault items you have stored and is known only to you, consistent with our *Trust No One* security model.

Trust No One

Trust No One is at the core of our security model and simply means that your secure data can't be retrieved by anyone but you; not even us here at IronStratus. We utilize SHA-2^v (SHA-512 to be exact) to securely store a one-way encrypted hash version of your main password in our secure IronStratus database in the cloud. However, no one, including IronStratus employees/developers, can retrieve or reconstruct your password. We've built the IronStratus service to be intrinsically secure so we don't have to rely on policies and procedure to keep your data secure, we simply can't access it, even if we were under a court order to do so!

When you first login to IronStratus, the IS browser add-on recalculates the one-way hash for your main login password and compares that to what is stored by IronStratus to authenticate you into your IronStratus account. All secure items that you add to your IronStratus vault are encrypted (we use AES-256 and your main login password is used as the key) locally by the IS add-on and are transferred over HTTPS and SSL and stored securely by the IronStratus server until needed. When you are logged in to your IronStratus account, you can get one-click login to any of the websites you have in your vault. The contents of your vault items are instantly retrieved and decrypted (locally in your browser) when you click on them, and injected into the target website login form.

Delegating access

Secure application access is obviously important for employees, but we often overlook our other business relationships that are more temporal in nature like contractors, temps, clients and partners. You also need a way to securely delegate or assign access to your accounts and applications on behalf of the company for these temporal workers to do their job or fulfill their partner obligations. This has typically been done by you emailing over a username and password (maybe even your username and password) for temporary access to the systems, applications and websites they need access to. But these relationships are typically pretty transient and the last thing your business needs is that person to still have access after they leave.

Access and all associated login credentials can be assigned and managed easily within IronStratus and you have the option of hiding the credentials when you share access so that the person receiving access will never know the credentials and you will be able to revoke access at any time. This is extremely useful for granting temporary access to critical resources for a project, for example.

Getting this type of security boost for your company doesn't have to be hard or expensive. You can sign-up for your own FREE IronStratus account in just 5-minutes at: <http://bit.ly/rpVNdv>

Portable, Secure & Convenient

IronStratus is a cloud application, so you can login to IronStratus from anywhere and have instant access to all of your business applications and accounts just by remembering one master password into IronStratus.

When logging on from computers other than your own, IronStratus automatically detects whether the browser has our add-on or not, and automatically installs it as necessary. While there is always some risk in using a computer that you don't own or control (e.g. someone could install something on a computer that tracks all key strokes), you can rest easy with the fact that IronStratus never leaves or stores any secure data in any form on the computer that you login in from (we do leave the browser add-on installed by default, but that does not have any secure information).

So whether you are at home or at work, on the road or on vacation, you can always securely access your key accounts and websites with IronStratus.

The Wrap up

Whether you access password protected websites for business or personal purposes, you owe it to yourself to educate yourself a little and have some awareness of what are the security risks and what are reasonable precautions to take. Like many things, security has many layers and it is very hard to eliminate all risk, regardless of precautions.

Most people place a lot of trust in the security provided by vendors for their computer operating system (Windows, Mac, etc.), their browser (Internet Explorer, Firefox, Chrome, etc.), or their network service (Cable, DSL, Wireless, etc.). Picking a secure login management product and creating and using many different and strong passwords is one of the lowest cost and highest returns ways you can protect your assets and make it harder for the bad guys to get access to things important to you and your business.

Here are a few security sites that we trust...

SecurityNews: <http://www.securitynewsdaily.com/security-tips-of-the-day-1192/>

OpenSecurityFoundation: <http://opensecurityfoundation.org/>

... and of course:

IronStratus: <http://www.ironstratus.com>

To sign-up for own FREE IronStratus account or get more IronStratus use cases, please check-out the IronStratus web site at www.ironstratus.com/what-we-do

ⁱ "The 10 Biggest Security Stories of 2011..." <http://bit.ly/wG9LBe>

ⁱⁱ Security breaches average \$7.2 per incident...<http://bloom.bg/wx3VZ4>

ⁱⁱⁱ GRC: Haystack site...<http://bit.ly/ykCsAy>

^{iv} OSF DataLossDB...<http://bit.ly/whYYNx>

^v SHA-2 Wikipedia definition...<http://bit.ly/yeEhJ>