YAHOO! omg!
MEXICO

Too many passwords to remember?

Innovation Jockeys Inspiration – jue, 27 jun 2013 13:03 CDT

You no longer need to remember multiple usernames and passwordsIn today's mobile world, we have access to numerous platforms, apps and even email accounts. This access demands creating multiple user names and with secure passwords. To add to the problem, reports of online identity theft and password hacking are on the rise, making secure access over the internet extremely critical. However, most of us either choose to keep the same password for all accounts or simple ones that are easy to remember, and just as easy to hack. So what is the solution?

The answer to the problem lies in Single Sign-On (SSO) solutions.

SmartSignin, a Toronto based company, provides one such cloud based SSO, Identity & Access Management solution with two-factor authentication. The service, launched in January, can perform one-click logins to all your websites and applications from a single secure portal. The company has its development center in New Delhi and a R&D wing at Ganita Labs, University of Toronto.

The SmartSignin Smart-Key (patent pending) algorithm will provide you with strong security by making sure that no one other than you can access your key. As the encryption and decryption is performed on your device, your usernames and passwords are not stored anywhere, wherein they can be stolen. The service also ensures that there is no single point-of-failure in the application.

An easy to use dashboard gives access to unlimited web-apps, with no collaboration required for third party and implementation is quick. The IAM (Identity and Access Management) Suite also offers customers a one-time SMS password, knowledge-based authentication (KBA, verification of previously submitted user information), along with the company's Smart-Key authentication method making the 2 step authentication process extremely secure. The service can communicate with popular applications across the web-space like Google Apps, SalesForce, and others.

With companies increasingly adopting the 'bring your own device' (BYOD) policy, employees are choosing to bring their personal devices to work. In such cases the platform also acts as a secure portal for mobile access from these devices. If an employee wants to access company resources from any device, they must authenticate through SmartSignin. Once connected, your company's policies can dictate how things go from there.

Forget the confusion of having to remember multiple passwords

Organizations with multiple departments need to provide different levels of access to their employees. In such situation, SmartSignin allows you to sync users and map their permissions across many popular applications. Simply create a user and assign the user to a group. He or she can then access the required applications by simply clicking on an icon on the desktop.

SmartSignin currently has over 7000 professional users, more than 16 small and medium businesses and 7 enterprise customers registered.

The company insists they are far more secure than their competitors who use server side encryption and store all client data to enable their technology to work. SmartSignin meanwhile, does not store anything that is not encrypted. The encryption they perform happens on the user side and the keys never leave the user's device.

SmartSignin also uses a cookie-less and token-less architecture in order to maintain complete privacy.