Ansys debuts Solid webKey for online passwords

Developed and designed in South Africa at digital technology solutions provider, Ansys' design and manufacturing facility, Solid webKey helps internet users to follow global best practices for protecting online accounts, in a simple-to-use but highly secure manner.

© bluebay via www.123RF.com

Thanks to its patented password protection technology, the Solid webKey all-in-one online password vault and security authentication product can generate and store long, unique passwords for every site you visit, while the owner only has to remember one master password themselves.

“Research performed on data which has been leaked onto the internet by criminal hackers continually shows that the general public struggles with basic account security,” explains Teddy Daka, CEO, Ansys. “Year after year, we see that easy to crack passwords such as ‘123456’ or ‘password’ are still in common use, and individuals rely on just one or two memorable passwords or passphrases to protect all their online accounts.”

Database of 30 million+ South Africans leaked online, property group is culprit

Ilse van den Berg 19 Oct 2017

Security experts recommend the use of long passwords made up of uncommon phrases, and that every account is protected with a unique password. Yet when millions of passwords lost in data leaks area analysed – including some of the three billion stolen from Yahoo! In 2013 – the same simple credentials are used over and over again. And if account name and password combinations details stolen from one service can be used to access another, the user is in trouble.

One significant challenge is that the best advice isn’t getting through to end-users. Many sites maintain outdated password policies which still require a mix of upper and lowercase, symbols and numbers. But even strong passphrases are impossible to remember without help, if a new one is created for every account. With Solid webKey, you can generate passwords that comply with any policy using the maximum length accepted by the application, without having to remember it.

How does it work?

Passwords are stored on flash memory on-board the physical Solid webKey device, which can be plugged into a USB port on any PC. Once plugged in, it synchronises with the Solid KeyPass software, which is derived from the industry-standard open source KeePass Password Safe, for access.

The product also has a unique and patented “liveliness” test as a second line of defence against loss of data, which requires a physical tap of the device before passwords can be accessed. This guards against the threat of malware which could steal passwords from the database after they have been decrypted.

South Africans easy meat for hackers

27 Sep 2017

Even strong passwords aren’t enough to defend against committed attackers, however, who may gain access to log-in credentials via phishing or other attacks.

To protect against this kind of threat, its second core feature is that it can also act as a hardware token for two-factor authentication (2FA), and is compatible with the Universal Two-Factor (U2F) standard promoted by the FIDO Alliance.

U2F is supported by popular service providers such as Google, Facebook and Dropbox. When enabled as an account setting, users will only be able to log in to these services when the Solid webKey is physically present and the device is tapped by the user.

Solid webKey will be available from 31 October 2017.