Australian Taxation Office fails to keep user passwords secure

/EINPresswire.com/ IT Governance, the global leader in information security book, tools and training, calls on organisations to address the startling holes in information security practices that saw the Australian Taxation Office (ATO) insecurely storing passwords.

A recent article on ZDNet revealed that the Australian Taxation Office (ATO) has been storing passwords in plain text. This insecure practice leaves unencrypted passwords, which people often use for multiple websites including transactional websites, vulnerable to hackers.

Best practice for the storage of password data is for passwords to be both hashed and salted. Hashing passwords is the encryption of the password by a hashing algorithm prior to storing the password in a database. Salting a password is the addition of random data to the hashed password where the resulting output, but not the original password, is stored in the database. When passwords are both hashed and salted they are much more secure.

Applying information security best practices to data, and in particular password data, will help to mitigate the risk of data loss, reduce damage to websites, and help to avoid user data being exploited.

Alan Calder, CEO of cyber security specialists IT Governance, wrote in his blog: "…It's time to go beyond passwords, to two-factor authentication and the more widespread use of software like Trusteer Rapport. While this is a logical direction of travel for organisations with deeper pockets (and we're seeing more and more of these sorts of solutions from online banking institutions), it's not so easy in the short term for individuals or most other organisations."

Calder adds, "For other organisations, staff training and awareness – ideally delivered within a structured ISO27001 Information Security Management System that enforces proper password selection and management – is the essential, immediate step…"

Organisations without an Information Security Management System (ISMS) are putting their livelihood at risk. An ISMS provides a systematic approach to managing confidential or sensitive corporate information so that it remains secure. It encompasses people, processes and IT systems.

The No 3 Comprehensive ISO27001 ISMS Toolkit (Download) offers organisations a way to develop an ISO27001-compliant ISMS through a comprehensive set of tools and materials. The toolkit accelerates your ISO27001 project through the combination of hundreds of pages of fit-for-purpose policies and procedures, books and tools. ISO27001 toolkits are indispensable for any organisation that intends to become ISO/IEC27001 certified.

The No 3 Comprehensive ISO27001 ISMS Toolkit (Download) is available for immediate download from: www.itgovernance.asia/p-919.aspx