

## Product Review: IronKey USB Memory and Encryption

"Laptop theft is the second most common computer crime and less than 2 percent of those stolen laptops are ever recovered", according to the Federal Trade Commission and the Federal Bureau of Investigations. "Four in five (81%) of US firms have had at least one laptop stolen containing sensitive information according to a recent study." In 2005, 32,771,838 and in 2006, 31,796,167, records were compromised when laptops were stolen from companies such as gas and energy, county, state and federal government agencies, retailers, colleges and universities, hospitals and banks. Well known corporate and government agencies top the list from the Veteran's Administration and Navy to the Bank of America. Laptop theft is not limited to businesses or organizations, but in many instances laptops are stolen from individuals. These individuals may be contractors for businesses or just someone like you or me, who use our laptop regularly. They can be stolen from offices, homes, cars, and during travel.

In 2008, the NIH had information from 2500 patients compromised with the loss of stolen laptops. In Nashville, TN some 337,000 resident's information became available for identity theft when county official realized that thieves had broken into the county building and stolen laptops. The cost to the county will include over 1 million dollars as they provide identity theft protection to those affected by the theft. There have been approximately 217 million records stolen in the past three years, 2005-2008, according to Paul Stevens, Director of Policy and Advocacy with Privacy Rights Clearinghouse (a private advocacy group).

Thefts of laptops occur all around the world. It was so serious in the United Kingdom that in January of 2008, The UK's Ministry of Defense began a review of information security policies after a stolen laptop resulted in a major security breach. The laptop, stolen from a vehicle used by a military recruitment officer, had information on approximately 600,000 people. Much of the information was basic contact information but for 153,000 individuals more sensitive information was exposed including passport information, National Health Services numbers, driver's license numbers and medical information. For an additional 3,700 people, financial and banking information had been stored on the laptop. To make matters worse, while all this confidential information was stored on the laptop, none of it was encrypted.

The information stored on both business and personal computers is not always limited to corporate information, but may include information such as personal, banking, credit card or investments. Also stores on many computers are account numbers, passwords and information on friends and family. When this data falls into the wrong hands it can be used to apply for any number of financial opportunities under false names by identity thieves.

Your laptop does not have to be stolen, to gain information. How long do you think it would take someone to access the information on our computer, by simply "borrowing" it, copy all of your information and return it? How often do we work on our computer completing on line bill payments and other personal "chores" in public such as the airport, coffee house, library or other places we happen to be? Identity thieves can have a great deal of information right at their fingertips as we leave our laptop open, work while sitting next to someone or forget to close windows or log out and secure our computer before we get up to get that second double espresso. How can we protect your laptop information and keep working anywhere and everywhere that we need to? IronKey offers a hardware-encrypted USB flash drive to protect your secure your most important portable data. No one can access the data on your IronKey if it is ever stolen, lost or "borrowed."

IronKey offers the following features: drive contents encrypted using AES CBC-mode encryption, a true random number generator for the maximum protection generates encryption keys in hardware, securely stores passwords, fast (30MBPS) read, fast (20MBPS) write, encased in a potted metal case- not plastic which makes it one of the strongest USB keys around, exceeds military waterproofing standards, and has the ability to safely tunnel through insecure wireless networks.

IronKey does not require software, drivers, or administrator privileges. When the US Military needed portable storage secured, IronKey is the technology they chose to use. IronKey passwords are super protected; after 10 incorrect password attempts, the encryption chip self-destructs, making the contents of the flash drive totally unreadable. Understand that the flash drive itself does not self-destruct but the encryption chop does so the contents are completely unreadable.

IronKey utilizes a precise die-casting metal process to construct the Iron Key's metal casing to exact specifications for thickness, strength and durability. Iron and other metals are used to make the strong metal shell. IronKey is waterproof and tamperproof. No one can tamper with an IronKey without destroying or causing irreparable and noticeable damage.

IronKey has distinguished itself from the competition in its features like encryption, secure browser, and overall security features. IronKey has products for personal or business use, from 1 GB up to 8 GB, with prices starting at \$79.99. IronKey is like a personal "Fort Knox" for college students, businesses or anyone who wants to protect their personal information and their identity.

## About the Author

Lisa Carey is a contributing author for [Identity Theft Secrets: prevention and protection](#). You can get tips on Identity theft protection, software, and monitoring your credit as well as learn more about the secrets used by identity thieves at the [Identity Theft Secrets blog](#).

Source: [www.isnare.com](http://www.isnare.com)

Source: <http://articles.exospy.com>