

Reston Firm Combats Identity Theft

By Gregg MacDonald

Thinking about throwing away, donating, or recycling an old computer? You might want to read this first.

According to Joseph Fergus, CEO of Reston-based nexGrën, simply “trashing” your computer files, reformatting your hard drive and reinstalling your computer’s operating system will not eliminate sensitive information hackers can use to steal your identity.

Fergus says that personal information such as photo files, credit card account numbers and bank account information can still remain on your computer in the form of magnetic “imprints” on your hard drive that are not erased by any of the measures mentioned above. “A lot of people do their taxes on their computers,” he said. “Imagine what sort of information that could provide to hackers hoping to steal your identity.”

In 2008, nearly 10 million Americans fell victim to identity theft and it has cost U.S. corporations more than \$60 billion over the last five years, the company said in a statement.

Additionally, consumer electronics disposal has become the fastest growing international “waste stream,” Fergus said.

According to an EPA study released in 2008, more than 65 million PCs and laptops are

disposed of each year, with an estimated 67 million more stored in offices and homes awaiting disposal, the company said in a statement.

In 2002, Fergus developed a “total-erase” data-removal software program for the Department of Defense. “Soldiers who had laptops in the

field were able to use it in case they had to drop their laptops in the course of saving their own lives,” he said.

Earlier this year, Fergus launched his new company, nexGrën (pronounced nex-green), with the goal of offering this same level of cyber security to everyone.

Developed as a version of the same patented and proprietary software technology used by the military, nexGrën’s “DiskEraser” removes every

file on a computer by writing random data on the entire hard drive, Fergus said. This leaves the drive and the system itself completely clean of any information. “It writes over any existing information, and renders any existing magnetic imprints illegible and useless for the purposes of identity theft,” he said. “It even erases information on image drives,” he added.

An image drive is an additional, “mirror-image” hard drive built in to certain operating systems such as Windows Vista, to allow disk backup or recovery in case of a fatal system failure on a computer.

“The permanent removal of sensitive, confidential information from a computer’s hard drive protects the consumer from identity theft and gives them peace of mind to donate, recycle or otherwise dispose of the device without fear of their sensitive information falling into the wrong hands. It also enables consumers to do their part to protect the environment.”

**Joseph Fergus
Founder & CEO
nexGrën, Inc.**

“The permanent removal of sensitive, confidential information from a computer’s hard drive protects the consumer from identity theft and gives them peace of mind to donate, recycle or otherwise dispose of the device without fear of their sensitive information falling into the wrong hands. It also enables consumers to do their part to protect the environment,” Fergus said in a statement.

According to Fergus, 81 percent of American households have a PC or laptop computer and an average of nearly 50 percent of those households have at least one non-working computer in a closet, basement or attic.

As part of nexGrēn’s planned business model, Fergus plans to soon initiate nationwide distribution centers where consumers can safely and securely recycle or dispose of their old computers. “We will guarantee that their data will not fall into the wrong hands,” he said.

In addition to being committed to providing a “green, efficient, secure” method of PC, laptop, PDA and cell phone disposal, Fergus hopes to also help stimulate the sagging economy.

“These distribution centers could also employ hundreds, if not thousands of people across the U.S.,” he said.