

Timothy Perrin

He Who Steals My Laptop Steals My Life!



In February of 2006, thieves broke into our van in Bilbao, Spain, and among other things stole our two laptop computers.

The theft itself was an irritation more than a tragedy. We didn't lose any significant data. I had been very good about backing up to a small, portable hard drive that I kept with me in a bellybag virtually all the time. We did lose a few days' worth of photographs, but that was about all.

In the end, the problem became not what we had lost but what the thieves had gained. It has been our great good fortune that we were the victims of amateurs who, after a year, apparently just don't know what to do with what they've found, because what they found was an identity thief's dream.

I try to run a paperless life. That means my filing system is scanning and shredding. As a result, the thieves have copies of all my credit card and bank statements for the last several years. Because I'm an amateur genealogist, they not only have my mother's maiden name, they have her mother's maiden name and her mother's maiden name and her mother's maiden name, back to the 16th century.

It took several hours on a friend's computer changing passwords and log-in IDs on dozens of online accounts, along with transatlantic phone calls, to cancel all our credit card companies—not just the two that were physically stolen.

In the end, we didn't lose any money and had very little hassle out of the whole thing.

I try to run a paperless life. That means my filing system is scanning and shredding.

But we were lucky. All we had on our computers was personal information. Imagine the problems if the thieves had gotten hold of dozens or even hundreds of client files.

In the United States, when a lawyer or Notary loses a computer containing client data, he or she is required by law to notify every client of the theft. As I write this, there is a law currently before Congress that would require the person to place ads in the local media attesting to his or her poor stewardship of confidential client information.

All this got me thinking, of course, about

(a) getting my laptop back if it were ever stolen again, and

(b) protecting my data.

Getting Your Laptop Back

According to the FBI, more dollars were lost in 2005 to laptop theft than any other computer crime, other than viruses. Your laptop has a 1 in 10 chance of being stolen this year and once it's gone, you have only a 3 percent chance of ever seeing it again.

A number of products are available to help improve those odds substantially. Some offer recovery rates as high as 95 percent. Virtually all operate in a similar fashion: your laptop "phones home"—the software company's security centre—whenever it is connected to the Internet.

If your laptop is stolen, besides calling the police, you notify the software company and they begin tracking your laptop. With this information, police are able to get search warrants for the location of your laptop. There is usually an arrest and your computer is returned.

Vancouver's Absolute Software Corporation is one of the leaders in this field. Its Computrace Lojack for Laptops (<http://www.lojackforlaptops.com>) usually can survive even a reformatting or repartitioning of your hard drive. On a Dell, Lenovo, Gateway, HP, and Fujitsu laptop, their software will embed itself into the BIOS and survive even the removal of the computer's hard drive.

I've written about LoJack for Laptops before in this space. I just wish I'd taken my own advice and bought it back then. You can rest assured it's installed on my replacement laptop.

<http://www.LojackforLaptops.com>

Protecting Your Data

But, in the end, a computer is just a pile of chips. It is only as valuable as the data it contains. The loss of the data can destroy your business—and the businesses of many of your clients.

If you think your computer is safe because you need a password or even a fingerprint to log into it, you're mistaken. I'll bet I can log on to any computer in your office right now and have complete access to all its files. All I need is a USB memory stick or CD version of Linux or Windows that can boot your system, completely sidestepping all the security features you've installed. Your precious data will be wide open. It doesn't take any expertise at all—just the right CD. I can even put a separate installation of Windows on a USB memory stick.

The only real solution is to encrypt your data.

Again, a BC company is one of the leaders in the field, this time a Kelowna company with the unlikely name of Frog and Tadpole Enterprises Inc., the brainchild of businesswoman Melody Zacharias and her husband Chris—he handles the marketing.

The company's APO Encryption product meets US, Canadian, and British military standards and makes your files impossible to read. In theory, a supercomputer could crack the code, but it would take it several thousand years.

The APO encryption package uses a random number-generator based on your last 20 or 30 mouse movements, along with your last few dozen keystrokes, to create encryption keys. In version 3 of the product, which should be released by the time you read this, the program will operate completely transparently. For example, you can designate that all Microsoft Word .DOC files are to be encrypted and they will be. You won't know that once you've entered the key, however.

And here's the good news. You don't have to remember any 40-digit pass phrases to make this system work. You can simply put the key file on a USB memory stick, the kind many of us have on our key chains. Plug the keychain plug into your computer and it will be as if nothing is encrypted at all. Without the USB memory stick, it's absolutely impossible to read any of the files.

Worried about losing that USB memory stick? You should be. "There is no backdoor in the software," says Chris Zacharias from Frog and Tadpole Enterprises. If you lose the key, you lose the files—permanently. That's why the manual warns you frequently and in bold red letters how to safeguard your key, how to back it up, and even suggests where to keep the backups.

For example, you might want to keep backups of your encryption keys—you can have several for different purposes—on a CD at home, another copy at work, and another copy in the safety deposit box at the bank.

If you use the server version of the company's software, it will generate one-time keys you can use to send documents to clients. Your clients can then use APO's free reader program to decode them—branded with your logo, by the way. That way, you can send highly confidential information over the Internet in complete security.

The single-user version of APO Encryption is only \$50. The Pro version, with some additional very useful convenience features, is \$75. The Enterprise version—including the ability to send those easily encrypted emails—is \$100. Server software is \$395.

<http://www.APOencryption.com> ▲

Tim Perrin has been writing this column since 1993. For the first 5 years, he was a lawyer in Vancouver and the BC Interior, then left the profession in 1998 to write and teach. Now he's returned to law with the firm of Bassett & Co. in Westbank, BC.
tperrin@OkanaganLaw.com

Thousands of BC Decision-Makers Read *The Scrivener!*

This magazine reaches the following spheres of influence, quarterly.

- BC Notaries
- Land Appraisers
- Land Surveyors of BC
- Lawyers
- Real Estate Professionals
- Real Estate Boards and Associations
- Provincial/Federal Court Judges
- Registrars
- MLAs and MPs
- Life Insurance Brokers and Agents
- Accountants
- Managers of Financial Institutions
- Mayors
- Government Ministries
- Libraries: Public and Private, including Law Society, Legal Services, Educational Facilities
- Investment Management Agencies
- Chambers of Commerce
- BC Housing
- BC Assessment
- BC Buildings Corporation

Advertising Deadline for the Summer Issue: May 15, 2007

Promote your services to our prequalified audience of Allied Professionals!

604 985-9250
scrivener@notaries.bc.ca