

Encryption: Why you should be using it.

by Bill Hely

Encryption is the process of turning ordinary text or images into a random, meaningless jumble of characters. Decryption is the reverse process, converting the encoded message back into its original form

At one time or another most businesses have a need to correspond confidentially, or to ensure the absolute security of important and/or sensitive data files.

Many private individuals find themselves with the same requirements.

However the general view of many security and law enforcement agencies has historically been that only unsavory characters such as pornographers, spies, drug dealers, terrorists, and other despicable types need to use encryption to protect their correspondence and computer files.

That's about as simplistic—and as wrong—as claiming that putting a letter in a sealed envelope, or putting a padlock on your back yard shed, is evidence that you are up to no good and have something to hide.

The real objection is that, while envelopes are easily slit open and bolt-cutters make short work of padlocks, secure encryption technologies are a very different proposition. Choose the right encryption solution and your “secrets” are, for all practical purposes, inviolate.

Security of communications is a very legitimate concern. Almost daily someone somewhere pays a high price for allowing sensitive correspondence to fall into unauthorized or undesirable hands.

There are many good reasons why ordinary law-abiding individuals might (and in fact should) use encryption. Here are some examples drawn from sources all over the World Wide Web:

- In the home, couples who share a PC can often view one another's eMail, yet they may have quite legitimate secrets from one another, such as plans for a birthday celebration, a surprise holiday, and so on.
- Lovers exchanging “sweet nothings” might want to encrypt them. To the lovers their words may seem only amorous. However certain others might view them as erotic or worse. Such “innocent” notes have resulted in court cases and dismissals, and should wisely be protected from the sight of others.
- Company policy should mandate the use of encryption in certain circumstances. For example, the development team for a new product should certainly encrypt all eMail regarding the product and the development process. Development plans, patent registrations, and plans for marketing, production, pricing, etc. should be securely protected. In this case not only should electronic correspondence be encrypted, but so should data files.
- Industrial action—the union perspective: In response to a strike by flight attendants, Northwest Airlines (USA) filed a lawsuit against the union. The company then obtained a court order to seize the personal computers of some employees so that files on the hard drives could be examined. The airline was looking for evidence that union leaders conspired to conduct a strike contrary to an existing labor contract. They were then able to browse through **all** files on each hard drive, not merely files related to the strike. Obviously, if you don't want your employer (or anyone else) to be able to browse files on your home PC, the files should be encrypted. It's too late to start erasing files when a

Encryption: Why you should be using it.

subpoena is thrust into your hand. And besides, erased files can usually be recovered fairly easily.

- Industrial action—the employer perspective: A large employer is involved in intense contract negotiations with the union representing hundreds of the company's employees. The CEO wants to instruct his negotiator regarding his absolute limit on salaries and benefits, while allowing the negotiator room to work out a better deal for the company if possible. Knowing that staff members surrounding him may be sympathetic to the union, the CEO removes temptation and ensures security by exchanging only encrypted eMail with the negotiator.
- A property developer is keen to build a new accommodation complex, but the land he needs is owned by four different parties. If his plans became known before he can purchase all four parcels, the price of each would skyrocket. eMail correspondence between the developer, his real estate broker, attorney, financial backers, etc. should be encrypted.
- Let's say a company is bidding on a major project. Members of the bidding team will often travel with laptops loaded with information pertinent to the bid, information which may include cost estimates, employees who will work on the project, technical specs, spreadsheets and so on. Critical stuff? Sure is, and you wouldn't want one of those laptops to fall into the wrong hands. Encrypt it.
- The CEOs of two corporations are discussing a merger. They exchange eMail messages, which must be kept from other companies that might want to interfere.
- A company is headhunting a key executive at another company, who doesn't want his current employer to know he may be leaving. Many employers routinely monitor eMail on their company computers, so messages exchanged during negotiations should be encrypted.
- If it is likely that you might want to talk to your bank or credit card issuer during business hours (while you are at work) it is a legitimate convenience to keep a file containing a list of cards, accounts, account numbers, issuers' phone numbers etc. on your work PC. Obviously this file needs to be encrypted.
- Priests, counselors, mentors, and the like sometimes counsel their charges via eMail. Such sensitive communications must be encrypted.
- In the aftermath of the 9/11 certain security and law enforcement agencies in several western democracies have the authority to intercept eMail messages without a search warrant. If this offends you, you definitely should encrypt your eMail.
- When your PC or laptop needs repair, are you OK with the service tech being able to browse all your personal and financial files?
- Anyone who provides information to a lawyer regarding a lawsuit or criminal case via eMail should use encryption to ensure confidentiality. With many security agencies listening to phone conversations between lawyers and their clients, preservation of attorney-client privilege can only be guaranteed by the use of encryption.
- Roman Catholic archbishop of Los Angeles Cardinal Roger Mahony, in some 60 eMail messages to the diocese's attorney, apparently admits prior knowledge of sexual molestations by priests, and even comments on a cover-up of the cases. His eMails were provided to a radio station and published in the *Los Angeles Times* in April 2002.

Encryption: Why you should be using it.

- *Los Angeles Times*, November 4, 2006: “Laptop seizure raises concerns over firms' data”. According to the article, agents of US Customs & Border Protection have the right not only to examine laptop computers carried by international travelers, including laptops carried by US citizens, but also to seize them, all without any warrants. While they are searching for threats, proprietary business data are placed at risk. Reportedly this is not peculiar to the United States. International travelers carrying a laptop should encrypt all files containing sensitive, confidential, or merely embarrassing data.
- The loss or theft of removable storage media is a recurring problem affecting financial institutions, government agencies, colleges, military and so on. Such loss may lead to the compromise of sensitive data and the possibility of identity theft and, in the case of military data, the compromise of national security.
- And so on. The quite legitimate variations are endless.

As you can see, there is nothing sinister about any citizen or business wanting to keep personal communications and information secret. It should be no more suspicious than sealing a personal letter into an envelope for posting, or locking the desk drawer where the checkbook is kept.

In today's paranoid world some regimes may view the mere use of encryption as evidence of wrong-doing. But just possibly the more widespread and routine use of encryption would temper such suspicions.

Today the communication medium of choice is eMail, yet even novice computer users are generally aware that eMail is inherently unsafe and prone to interception and eavesdropping—particularly in a corporate environment, where all message traffic may pass through an in-house Server.

The only viable, universally applicable solution to securing electronic communications is encryption. Unfortunately that solution has often been considered and quickly abandoned because it can be quite difficult for non-experts to understand, implement and use.

After much searching and testing, the encryption software I eventually selected for myself and my clients is both inexpensive and very easy to come to grips with, and is ideal for use as either a business or personal encryption tool.

You can download a free, yet still full-featured, 15-day trial from here:

<http://HackersNightmare.com/FAOPGP>

To get the trial, first read that page then click on the Downloads menu option. Don't be confused by all the other specialist packages on offer; the one you want is *FileAssurity OpenPGP*. Don't choose the “*Lite*” version either, as it is lacking in some important and very useful features.

To help those new to encryption to come to grips with the application as quickly as possible, I wrote a step-by-step tutorial booklet that will have you using industrial strength encryption like an old pro on a single read-through.

Called “*Code Rings & Secret Handshakes: Practical encryption for beginners*”, it's a step-by-step treatment of encryption, presented in simple terms, that requires no expert knowledge to implement.

Encryption: Why you should be using it.

The booklet takes a “programmed instruction” approach, so there is nothing to “learn”, just a number of clearly explained steps to follow. By working your way through the guide and following the steps just once, you should attain the competence to continue to use encryption easily and instinctively thereafter.

I recommend you use the booklet in conjunction with the free trial software to quickly determine if encryption is something you should be using, and to see for yourself just how easy it can be.

You can get the booklet from the link below as a PDF file, but be quick. The book is normally priced at \$47, but for a limited time it’s just \$7 to readers of these articles. You’ll find this special price available at:

<http://HackersNightmare.com/Encryption>

NOTE: Before you purchase my encryption guide, consider another option. Buyers of *The Hacker’s Nightmare*™ get the “*Code Rings & Secret Handshakes*” booklet as a free bonus.

-oOOo-

Bill Hely is a technologist, consultant and author living in Brisbane, Australia. For most of the last two decades his professional focus has been on advising and supporting small business operators in Information Technology and Office Productivity issues. He is the author of several books on technology for the business operator, including the Bible of Internet and computer security *The Hacker’s Nightmare*™.

To comment on this article please use the “Support” link at the bottom of the <http://HackersNightmare.com> main page.

Comments, suggestions, expressions of appreciation
— and especially testimonials —
are most welcome.