NO STARCH
PRESS

FOR IMMEDIATE RELEASE

Media contact: Patricia Witkin
patricia@nostarch.com
415.863.9900 x303

NEW BOOK PROVIDES SIMPLE SOLUTIONS FOR COMMUNICATING SECURELY WITH PGP

A straightforward guide to a complex topic: how to encrypt email with PGP or GPG

April 6, 2006, San Francisco—In today's world of electronic eavesdropping and computer security breaches, who isn't a little paranoid? The fact is, email isn't private. Any number of people can view your email, whether that someone is working at your ISP, working in your office, or sniffing your communications on the wire. When sending sensitive communications, such as credit card numbers, medical history, or even simple personal or family information, it's critical that you take steps to protect yourself.

One of the best ways to protect the privacy of email communications is to use PGP (pretty good privacy) and the Open Source GPG. Unfortunately, even hardcore geeks sometimes find PGP difficult to set up, configure, use, and troubleshoot. Recognizing this problem, No Starch Press has published a simple guide to using PGP and GPG. In **PGP & GPG: Email for the Practical Paranoid** (No Starch Press, April 2006), author Michael Lucas offers an easy-to-read, informal tutorial for communicating securely with PGP.

PGP & GPG: Email for the Practical Paranoid explains how PGP works, and how to integrate it into the most common email clients, including Outlook and Mozilla's Thunderbird. Lucas tells how to use the tricky command-line versions of PGP, and walks the reader through using PGP and GPG in daily email correspondence.

PGP & GPG is written for moderately skilled computer users who may be unfamiliar with public-key cryptography but who would like to protect their communications. Highlights include:

- A concentration on real-world usage instead of mathematical theory
- Instructions for installing and using PGP and GPG with Microsoft Outlook and Mozilla's Thunderbird
- Help with the tricky command-line versions of these programs
- What to do at a key-signing party, how to generate and manage your keys, and even how to add photos to your key

"Do the initials NSA mean anything to you? Do I have to use the word 'wiretapping' to make the relevance of PGP clear? Lots of people (like me) live their lives on email, and they need to be aware of the risks," said Bill Pollock, founder of No Starch Press. "Email is not secure unless you use PGP."

PGP & GPG: Email for the Practical Paranoid allows anyone to protect their personal data with free tools.

ABOUT THE AUTHOR: Michael W. Lucas is a network/security engineer with extensive experience working with high-availability systems. He is the author of the critically acclaimed *Absolute BSD*, *Absolute OpenBSD*, and *Cisco Routers for the Desperate* (all No Starch Press).

PGP & GPG: Email for the Practical Paranoid by Michael Lucas
April 2006, 216 pp., 2-color, $24.95, ISBN 1-59327-071-2
Available at fine bookstores everywhere, from www.oreilly.com/nostarch, or directly from No Starch Press (www.nostarch.com, orders@nostarch.com, 800.420.7240).

ABOUT NO STARCH PRESS: Founded in 1994, No Starch Press is one of the few remaining independent computer book publishers. We publish the finest in geek entertainment—unique books on technology, with a focus on Open Source, security, hacking, programming, and alternative operating systems. Our titles have personality, our authors are passionate, and our books tackle topics that people care about. See www.nostarch.com for more. (And by the way, most No Starch Press books use RepKover, a lay-flat binding that won't snap shut.)

# # #