New tools and strategies for engaging people in protecting the environment

Encrypting your email with PGP

PGP integrates seamlessly into Eudora (light and pro) and Microsoft Outlook, making it possible to easily and automatically handle the encryption process. If both you and the recipient of your message have PGP installed, PGP makes it impossible for anyone other than the intended recipient to decode your message in transit.

Why use encryption?

Although the **risk of your email being intercepted is low**--it's far easier and more rewarding to break into the typical conservation office than to snoop on their email--as we increase our use of online communications, and begin to win battles because of online networking, the **risks can only increase**. Encrypting your messages means that no-one other than the intended recipient can read your messages, and the widespread use of PGP encryption will help **deter the bad guys from thinking about trying to snoop** on us electronically. Another concern is the potentially indefinite life of a given email message; mail is routinely archived by ISPs and is **potentially subject to subpoena**. (This has not to our knowledge ever happened to a conservation--yet.) Also worrisome is the fact that the FBI possesses a tool called "Carnivore" that can, with a court order, be used to scan email at the ISP level. Privacy advocates have criticized this system as being indiscriminate and invasive. Encryption can help secure you against these intrusions.

PGP also allows you to "digitally sign" messages, allowing you to prove that you are the author of a given message. If you routinely sign all of your mail with PGP, it becomes possible for you to plausibly deny having written a message that lacks your digital signature.

More importantly, using encryption is an important assertion of your **fundamental right to online privacy**--a right that is increasingly under attack from a variety of directions. Using encryption doesn't mean you have something to hide; it means that the content of your messages is your business, and no-one else's. You don't send your letters on postcards for the world to see--you put them in sealed envelopes. **Routine use of encryption is like the routine use of envelopes**--there's nothing shady or suspicious about it.

ONE/Northwest's attitude on the routine use of encryption has until now been "wait and see." Although powerful encryption tools have been available for several years, we did not feel that they were sufficiently user-friendly for typical conservation activists to use. With current versions, we feel that email encryption software is now easy and convenient for routine use by activists concerned about the privacy of their email.

Two caveats:>

1) PGP is only effective if both sender and recipient have PGP software installed.

2) PGP cannot effectively encrypt messages distributed via email lists.

How does PGP work?

PGP is based on an encryption scheme known as "public key cryptography." Each user generates a unique "key" which is split into two parts: a "public" key, which is distributed widely, and a "private" key, for the user only. Each half of the key unlocks messages encrypted with the other half. So, when you want to send a secure message to someone, you encrypt the message using the recipient's public key. Only they have their private key, so only they will be able to decrypt the message. Similarly, public key cryptography allows you to digitally "sign" your message with your private key. Anyone will be able to decrypt it with your public key, but doing so will verify you as the authentic sender of the message.

For more details on how public key cryptography, check out the Tom McCune's "PGP Questions and

Answers" at:

For more information on online security in general, including email security, see our document "Online Security" at

What to do

In order to use PGP encryption, both sender and recipient must have PGP software. If someone does not have the software, and has not generated and distributed a public key, you cannot send encrypted email to that person. Therefore, ONE/Northwest recommends that you:

- **Download and install PGP freeware** from the MIT PGP Distribution Web site. Get everyone else you work with to do the same.
- Upgrade to a current version of an **email program that supports PGP plugins**. Email programs that support PGP include: Microsoft Outlook 97/98/2000, Microsoft Outlook Express 4.x/5.x, Qualcomm Eudora 4.x/5.x and Claris Emailer 2.x.

- Generate a public key, and allow PGP to **publish your key to a public keyserver**, where others can find it by using your email address. You can find out more about how to distribute your public key in the PGP documentation.

- Begin using PGP to **encrypt all of your person-to-person email with others who have PGP**. Unfortunately, **you cannot use PGP to encrypt mail sent to a majordomo email list**, such as those hosted by ONE/Northwest. As with all unencrypted email, you should continue to assume that anything posted to an email list could potentially be read by anyone.

Strong encryption is a technically complicated and politically charged subject. If you want more information, the PGPi Web site provides a great deal of useful information, and many links to other sources.

One last word: Encryption is probably not needed by most people in the Northwest conservation community, for most of their email communication. While it is *technically* possible to intercept email messages, it is not a trivial thing to do, and we don't feel that the threat to the bulk of our communication is great.

For more information

PGP Freeware download site
        http://web.mit.edu/network/pgp.html
PGPi.org reference site for PGP freeware
        http://www.pgpi.org
Tom McCune's "PGP Questions and Answers"
        http://www.mccune.cc/PGPpage2.htm

Related Articles

Online Security
        http://www.onenw.org/toolkit/security_final.html

Add Comment