REMAILERS

Traveling through the Internet, every email accumulates the trails of every machine it passes, along with the date, time and IP. Since this "post stamp" is rather unsightly and useless for correspondents, email programs normally hide it. But it's very easy to trace a message back to its author by reading these headers.

There are several ways to deal with headers and hide yourself. The best is to use Anonymous Remailers. A remailer is an address through which an electronic message passes before continuing the rest of its journey to its actual destination. It wipes out all the headers that can disclose your identity.

There are various remailer systems. Some systems give you an anonymous address on which other people can send you mail, which is then forwarded to your real address (so-called "pseudo-anonymous"). They keep the database of "real names" so you can be potentially traced back or the owner can be forced to give this information away. The rest of remailers act using "fire and forget" principle and keep no logs.

In fact, nowadays there are two different classes of remailers: Cypherpunk and Mixmaster.

Most of remailers use encryption.

Cypherpunk

On the first step in the evolution of really anonymous remailers ware Cypherpunk Remailers, also called "Type I" remailers. With a Type I protocol, a single message is forwarded between several systems before reaching its destination and has its identity stripped at each link. Moreover, and perhaps even more important, Type I remailers never create a database of identities.
According to the Type I protocol, a user must construct a chain of remailers, encrypting a message in a separate layer for each remailer. Each remailer publishes a PGP public key that users may use for an encryption layer. When a Cypherpunk remailer receives a message, it strips off a layer using its own private key, finding the identity of the next remailer within the decrypted bundle. Each remailer is able to decrypt the bundle it receives but it cannot itself look more than one link ahead (the one it should forward the message to), let alone determine the final destination. Moreover, after the first link the sender's identity is removed: the first link only knows the sender, and learns it not from anything in the bundle, but from who sent the bundle in the first place.

Mixmaster

Mixmasters are "Type II" remailers. They go one step further in the evolution by assuming that every network connection is being monitored. In order to protect email from those with the computing resources to monitor all network traffic, Mixmaster creates specific mechanisms to overcome agents studying traffic patterns. These mechanisms include reordering and message padding. Rather than simply forwarding each package to the next link as soon as it is received, a Mixmaster node will save messages for variable durations, bundling collections of messages together for transmission to a downstream node. So, type II remailers are much more resistant to traffic analysis, unreliable nodes, and other attacks than Type I remailers are.

"That's very nice, but I'm not a computer guru!"

It may seem that the actual, everyday use of remailers is difficult. But this is hardly the case! In fact, remailers are very easy to use thanks to a number of client front-ends available for several computer platforms.

Web remailers are quite nice if you need easy, "one click" privacy mail. Such pages permit you sending emails via anonymous remailing net without using a specific client

Remailers Tips

Use client-based remailers.

Web-based remailers are not as secure as client based ones because the encryption process goes on the remote server and not on your computer.

Use secure connections for web remailers.

Make sure that you use a secure connection (if possible) to compose and send messages. Unless you take precautions, your message and the final recipient will be sent unencrypted to the webserver where the remailer is based, so, anyone listening in on your connection to the server could know what and to whom you are mailing. To avoid this you should make sure that your web browser has 128 bit SSL Encryption and connect to one of the web remailers that uses a connection with SSL encryption.

Use PGP for type I remailers.

Encrypting outgoing message with the Cypherpunk remailer's public key is a simple and efficient way to increase you privacy. This can be done with any text editor like Notepad and a properly installed version of PGP. Keep in mind, too, that there are currently only a few Cypherpunk (Type I) remailers that will accept non-PGP messages and their number is dwindling.

Use chaining.

Since your message must enter the remailer network at some point, that first remailer operator can always know where the message is really coming from. The operator knows as much about you as can be revealed from your email headers. But if your message is chained to another remailer and encrypted with that remailer's key, then the first remailer and anyone snooping its traffic cannot read your message.