

## This e-mail will self-destruct in – oh, it's gone



**PAUL TAYLOR**  
PERSONAL TECHNOLOGY

In the late 1960s, Mission Impossible introduced millions of TV viewers to the idea of self-destructing tape messages.

Now, 40 years later, cunning minds at Void Communications have come up with the electronic equivalent – recordless e-mail messages that “vaporise” after being looked at. Void launched VaporStream this year to provide a secure way for business people to communicate without leaving an electronic trail to be picked up by snoops.

The \$40-a-year service ([www.vaporstream.com](http://www.vaporstream.com)) is a web-based online communications service that is like a cross between e-mail and IM (instant messaging) to use.

What makes “stream messaging” different is that it leaves no record on any computer or server while using existing e-mail addresses. Messages cannot be forwarded, edited, saved or printed.

The VaporStream network separates the sender's and receiver's names and the date from the body of the message so they are never seen together. Both sender and receiver must subscribe.

Here is how it works. Enter a

recipient's e-mail address and it disappears before you start typing the main body or message stream. On being sent, the message goes into a temporary storage buffer space. When the recipient calls up the message in the VaporStream in-tray, it is removed from the buffer space. The name and e-mail address of the sender vanish before the body appears. A VaporStream message can be looked at once before disappearing without trace.

There are limitations. For example, VaporStream subscribers can send only plain text messages. VaporStream is designed to complement e-mail and is aimed primarily at corporate users.

Its developers say it is ideal for ensuring that sensitive internal information stays confidential, for example on delicate issues such as human resources, medical matters and intellectual property.

Messages and headers are never hosted on the subscribing companies' networks, eliminating the risk that employers could intercept their employees' stream messages. Advocates claim it could, therefore, help reduce the corporate risk and liability associated with e-mail systems that record every message.

However, the service is not appropriate for, say, Wall Street brokerages or any other organisation required by regulators to record all electronic communications and produce them on request.

### THE BREAKDOWN

#### VAPORSTREAM

Pros: Recordless messaging that leaves no trail  
Cons: Not appropriate for everyone

#### ECHOWORX

Pros: Easy to use, highly secure encrypted e-mail for everyone  
Cons: Individuals must sign up through ISP

Can unsavoury individuals – or even terrorists – use VaporStream? Void emphasises that, as a US-based company, it complies with all US laws and regulations, and can be required by security forces to allow monitoring of VaporStream messages.

For the moment, VaporStream is available only to desktop users but Void plans to develop versions for Research In Motion's BlackBerry devices and Microsoft's Windows Mobile operating system so smartphone mobile subscribers will be able to access it.

For e-mail users who want to store e-mails but make them more secure, the obvious solution is encryption. But most e-mail encryption systems so far have been too complex for most users.

Now Canada-based Echoworx has developed an easy way for e-mail users to protect messages from prying eyes. Unlike

other such e-mail security systems I have tried, its Secure Mail is simple to install, quick and easy to use and requires no technical expertise.

Secure Mail allows subscribers to use existing e-mail applications, such as Microsoft Outlook and Outlook Express, to digitally sign, encrypt and decrypt e-mail messages on the desktop. Think of it as a digital “tamper-proof” envelope for e-mails. No extra software or hardware is required.

The service, which is sold through ISPs and telecommunications companies (mostly in the US), typically charges consumers \$5 to \$8 a month ([www.echoworx.com](http://www.echoworx.com)).

To send a secure message, the subscriber clicks the “secure” button, types in a password and presses send. The digitally signed and encrypted e-mail, plus any attachments, is sent to the recipient, who sees a gold lock next to the message in the inbox.

If the recipient is also a subscriber, they just type in their password to open the encrypted e-mail. If not, they are directed to a secure website where they are asked to answer a question agreed with the sender.

The Secure Mail service will appeal particularly to individuals concerned about identity theft or the privacy of their e-mail messages, but Echoworx also offers a business version.

Either way, Echoworx is worth a look.