How to hide emails from government snooping

Despite coalition proposals to monitor public email, there remain numerous free or low-cost methods to keep messages private

Email snooping can be avoided by solutions from encryption to anonymous remailing services. Photograph: NetPhotos/Alamy

You already know how to keep messages private: you just encrypt the contents using a password. But although this kind of technology has been freely available to PC users since Phil Zimmermann launched PGP (Pretty Good Privacy) in 1991, hardly anyone uses it. The benefits of email and online messaging are that they are fast and relatively frictionless – you don't need to address an envelope, find a stamp, walk to a post box and so on – and encryption becomes an annoyance.

The problem with the latest government attempts at snooping is that they are not concerned with the content of messages, but their existence. If you have found some suspected criminals or terrorists, then you will want to know who their friends are: the people they email or message most frequently. Each of these people can probably be identified by their internet protocol (IP) address: the number assigned by their ISP (internet service provider). Even an encrypted email will usually include the addresses of the sender and the recipient in its headers.

The general solution to privacy concerns is to use a non-UK "proxy server" to relay web pages, messages, anonymous email accounts and other content anonymously. Hackers who really want to hide their origins will use several proxy servers, including ones that are acting as proxies without their owner's knowledge. Many websites publish lists of free proxy servers, which are updated continuously.

Of course, these servers may offer less privacy than your ISP, and some may be traps or "honeypots". However, there are some trusted anonymous servers available either free or for modest payments.

Examples include hidemyass.com, anonymouse.org, Guardster, Proxify, IDzap and Megaproxy. Such servers usually have terms of service to prevent abusive or criminal behaviour. They will probably record your IP address and may report you if you breach them, so they're not completely beyond government reach. However, they're probably beyond government fishing expeditions.

There are also some really anonymous remailer services, which use networks such as Cypherpunk and Mixmaster to ensure privacy. The drawback is that if you send an email anonymously, the recipient cannot simply hit Reply. QuickSilver software for 32-bit Microsoft Windows makes it relatively simple to route an email through 45 or more remailers using Mixmaster. But like the Tor anonymous network, this kind of thing is mostly used by programmers and geeks.

There are simpler ways to send private and/or anonymous emails. For example, anonymouse.org offers a simple form for AnonEmail, as does the sendanonymousemail.net website. There's also Mailinator, which provides free disposable email addresses, and Hushmail, which works like an ordinary email service but encrypts all your email.

For encrypted instant messaging, you could try BitWiseIM or ProjectSCIM (for Secure Cryptographic Instant Messenger). Facebook's internal messaging is reasonably private because it's not visible on the net, though it could be vulnerable to a court order.

In the end, the simplest way to increase your privacy and security is to restrict your internet use to sites and services that have SSL connections. These are already standard for banks and shopping sites, and are increasingly used for email and other purposes. You can recognise them by the s for secure in their https: addresses, and a padlock visible in the browser. The next step is to use the InPrivate, Incognito or Private Browsing feature of your web browser to use anonymous online services.

However, it's worth trying proxy servers and services, if only to provide a nice illustration of the law of unintended consequences. In other words, government attempts to snoop can help to create an internet culture where snooping becomes impossible.