

UnderstandIT

From **MAY DAY CONSULTING LIMITED** in association with **Facilitators International LLP**

A publication designed to inform and enable businesses to understand the implications, costs and advantages of using Information and Communications Technology. Distributed through Chambers of Commerce.

LOCATING YOU AND YOUR BROWSER

The Mozilla Foundation is currently working on preparing to launch its latest version of Firefox, the web browser that has been so successful in breaking the virtual monopoly of Internet Explorer over the past couple of years.

At the same time, Mozilla has announced that future versions of the browser will include code based on a new application specification that is able to pinpoint the geographic location of the computer.

Therefore if you are a mobile Internet user, perhaps in an unfamiliar city or other location, then the browser will be able to provide you with information relevant to the location that you are in. This could include links to local services and businesses or perhaps "local" news that really is local to where you are at the time.

The application specification that will be used by Mozilla has been developed by the international World Wide Web Consortium (known as W3C), who develop and publish web standards and guidelines.

In order for advanced users to try out this new technology, Mozilla are promoting the use of an add-on feature called Geode (a third party application), that uses an early version of the new geo-location application. It uses WiFi to provide location information, and will therefore only work with laptops or other mobile devices using WiFi. However, it does point the way for future methods of making web browsing more relevant to the users' needs.

Some would argue that these developments could have perhaps sinister implications or at least infringe personal privacy. This concern is an increasing trend within this area of technology. Take the recent furore over PHORM (see previous editions of Understand IT for more information).

Privacy is likely to continue to be a serious concern of those trying to protect our rights to privacy. However, Geode and any future implementations of the geo-location specification within Firefox are stressing the safeguards that will be built into these facilities.

It is likely that most users will only seriously use such add-on features that guarantee that their privacy is protected. It will have to be clearly possible to opt-out completely from the feature, or at the very least decide just what information is used to identify exactly where you are, and of course will insist that any intermediate system will not store any personally identifiable information about users!

EMAIL ENCRYPTION

This subject has been on a wish-list of topics to be covered here in the pages of *Understand IT* for sometime. If you consider that the content of your business or personal emails is important enough to warrant encryption, then read on. The problem is that it can be a complex subject, with many different angles and a somewhat difficult topic to cover in a short space. However, given the importance of security of both personal and commercial information in this technology driven world, we are making a start here.

Having said this it is paradoxical that there does seem to be a lack of current development in this area, with much of what is available now becoming quite aged, having been pushed into the background by tools and solutions to protect individuals and businesses from web threats like phishing, viruses/Trojans and identity theft.

It should also be stated here that much of the encryption technology that is commercially available will provide an adequate level of protection from snooping by individuals and others, but would not stand up to the efforts of governments and national security organisations who have huge super-computers dedicated to beating any attempts at encryption.

The method used to ensure that your mail is encrypted securely will depend largely on the facilities that you use to send and receive email:

PC-based email client software

This software includes Microsoft Outlook, Outlook Express, or Mozilla Thunderbird or any one of a number of other programs - where the method used will be PC-based (obviously). These programs send mail and retrieve mail directly to the inbox/outbox located on your PC.

Web-based email

If, however, you use a web-based email service (Google mail, Hotmail, AOL or Yahoo mail for example), then it is likely that you will need to rely on the encryption facilities (if any!) provided by that particular mail service.

Web-based email services maintain your inbox, outbox and other folders on their own server(s), and you can access them wherever you may be, and copies of your mail are not normally stored on your local PC at all.

In order to have encryption available for web-based services, it is also likely that you will need to upgrade your email to an enhanced, chargeable service, principally aimed at businesses.

For the individual or small business, there are a number of encryption facilities that have been developed by individual encryption enthusiasts that are designed to provide a certain level of encryption to text in email messages or other documents. However, using these “scripts” is not straight-forward, usually requiring some technical skill and the resilience of the encryption method used is not necessarily robust.

For the sake of this article, we will concentrate on encryption of mail for those using a **PC-based client mail program** - although this can still be quite complex, depending on which approach is used.

When using a PC package like Outlook, there are essentially a couple of approaches to encryption – one that involves you registering and receiving encryption keys that are managed by you to encrypt messages after authenticating yourself to the local encryption software. This approach has its roots in the earlier attempts at providing encryption and many such facilities were free.

Alternative approaches now gaining favour are either to leave the encryption to software installed on your computer, which simplifies the process, or using online authentication with the supplier’s server to provide the authentication and the local encryption and decryption. These approaches to encryption are gaining more interest since they are easier to use, but tend to cost more.

Encryption keys

We start by apologising for becoming a little technical in order to explain the concept of keys, but it is useful for you to understand the basics of encryption in this context, since keys are essentially used in all forms of encryption.

There are normally 2 keys used to encrypt/decrypt your email text – a “public” key that is published by you to your correspondents at large, and a “private” key that is retained and must be kept totally secure by you. To encrypt or de-crypt the text of any message, you must have both keys available.

Your correspondent must also have enabled encryption and have his/her own public and private keys available.

PGP (Pretty Good Privacy)

One of the earliest organisations in this field was Pretty Good Privacy (PGP), which was originally set up by enthusiasts and provided registration and maintenance of keys for free. However, today it has become more of a mainstream commercial organisation and has developed packaged applications to simplify the encryption process, but you now also need to pay for their services.

In the case of PGP, once the software package you have selected (see below) is installed and configured (you will still need to understand the concept of public and private keys), much of the encryption and decryption is done behind the scenes and work can usually continue unchanged.

Your message created in any one of the supported email client software packages will be encrypted and will appear as an undecipherable series of hexadecimal characters if viewed by anyone en-route. Your correspondent must have the same encryption software installed and the email will be decrypted automatically. The often complex matter of using keys to encrypt and decrypt text as required by older (free) utilities are now hidden away.

One of PGP’s latest offerings is **PGP Desktop Email** for businesses/professionals. This application, which costs US\$74 for a one year subscription or US\$179 for a perpetual licence (per user) provides end to end encryption of your emails.

Alternatively there is the **PGP Desktop Home** offering for individuals at US\$119 for a perpetual licence.

Both products offer not only email encryption but some hard disk file encryption facilities including zip and other archive files.

More information can be found here:

http://row.store.pgp.com/desktop_email.html#

or

http://row.store.pgp.com/desktop_home.html

Managed Services

Another form of email encryption is the managed service whereby the encryption service provider maintains a database of subscribers and their authentication details. When a message is created and encrypted (using a small PC-based program) and you are authenticated online, the email is transmitted in its encrypted form. The recipient then has to authenticate him/herself to the same online server and the message is then decrypted.

One provider of this type of service is Ceelox:

Ceelox Securemail – MS Outlook add-on – able to use biometric verification of identity if available. Cost: US\$120 per user (2 year licence)

More info:

<http://www.ceelox.com/ceeloxsecuremail.html?gclid=CJ7FwPGR2JYCFQf8bgodmFBV3A#>

If you require more help on email or any other form of encryption, then please contact Alan Finch on (01224) 697457.

We wish to acknowledge with thanks that some of the material contained within this publication has been sourced from Computer Weekly, PC Pro, BBC and other reputable sources..

May Day Consulting Limited and your Chamber of Commerce have endeavoured to ensure the accuracy of the information contained in this publication, but do not accept liability for any inaccuracy or omission contained within it.

Information on other Business and IT services can be found on our web site at: <http://www.maydayconsulting.co.uk> or by calling Alan Finch on 07968 262079.

May Day Consulting Ltd

.....stress free IT

9 Benbecula Road
ABERDEEN AB16 1FT
Tel: (01224) 697457

E-mail: info@maydayconsulting.co.uk
Internet: <http://www.maydayconsulting.co.uk>