

Email encryption, the options

There have been email encryption solutions available for many years now. However, they have not generally been suitable for small to medium sized organizations – mostly due to set up and maintenance costs, and the in-house technical know-how required. This is why email encryption has remained a service that only enterprise level organisations have been able to offer but what are the options now?

With the rapidly increasing need for total email security many companies offering Software as a Service (SaaS) relays for anti-virus and anti-spam have branched out into email encryption by adapting existing systems. Many problems and vulnerabilities can develop from this approach.

TLS (Transport Layer Security)

Some companies providing SaaS will offer you encryption using TLS through them as a mediator. Your email server connects to them on an encrypted channel – this is called TLS. You send the mediator your email and although the channel of communication is encrypted, the actual email is not – the mediator gets your email in an unencrypted form.

The mediator can then forward your email onto your recipient's email server using TLS, but only if it is set up to offer TLS – many are not. If TLS is not offered by your recipient's email server then the email will either not be sent, or it will be sent insecurely along the second leg of its journey. This whole process is still vulnerable to "man-in-the-middle" attacks on both legs of the journey unless **both** sender and recipient pay for a trusted 3rd party authenticated certificate which costs in excess of 600 GBP a year. This is in addition to anything you pay for your "encryption service". If your recipient uses an anti-spam/anti-virus relay of their own, then even if the mediator connects to their relay securely, the relay might not connect to the recipient securely, making the whole process pointless once again.

Password protection

These "mediators" can generally offer to password protect emails you send recipients without the above facilities. The recipient registers a password with your mediator and when you send that recipient an email; your mediator will encrypt the email using their password. However, unless that password is very long and very complex it can be easily compromised. Most people do not use a long or complex password, which makes the process rather futile. Also, this method does not offer your contact the opportunity to reply securely or send you emails encrypted!

Portal based

The other method of secure messaging which a mediator might offer you is for your recipient to use a portal. Every time you send a specified recipient an email they will receive a notification of this via email – they will not get the actual email itself. They will then have to use a portal to log on and retrieve their message. Although this process is generally secure, it is cumbersome, time consuming and not very popular. It defeats the purpose of email.

Secure-mail

Secure-mail doesn't have any of these issues and its simple pricing, easy installation and zero maintenance mean that it is by far the most effective email encryption for SMEs.

Since Secure-mail is fully automated there isn't the challenge of training your staff to email securely – the way you email remains exactly the same. Also, **you are able to offer all of your contacts fully effective encryption for the emails they receive from you and send to you** – they don't log onto portals or register passwords; they just use their own email. This is why we believe Secure-mail is the best method of email encryption.