Email security for counsellors

With the increasing use of online counselling within student counselling services, preserving confidentiality is a major concern. **Stephen Allsopp** explains how sending an email is the equivalent of sending an unsealed letter in the post – and what can be done about it

Before we get into the details, it might be useful to give a very brief overview of how email works.

Most of us will be writing our emails using something like Outlook or Thunderbird. These are software programmes that take care of the details of storing and writing email messages, and maintaining address books, but they all essentially do the same jobs: collecting your email, filing it in folders, allowing you to write messages, and dealing with sending them out.

When you write an email, it is stored locally and then sent via an email server, which uses various configuration settings to work out where to send it to. Eventually, your message will reach its destination via a chain of servers, before being deposited onto the machine from which your recipient will be able to collect it using their email programme.

An email is, in its simplest form, just a simple piece of plain text. Some email will be formatted, but the important thing to remember is that your email is readable by anyone with access to it. It is the equivalent of sending a letter through the post in an unsealed envelope: at any stage in the delivery process, anyone who has access to it can look at it and read the contents.

So why bother?

As counsellors, we take it for granted that we do not leave our notes around where someone might be able to get hold of them. We use basic security precautions like locked filing cabinets, and separating identifying details from our notes to make sure that some measure of confidentiality and anonymity prevails. Generally, we try to make sure that the level of security is proportionate, so as to balance the level of risk of breach of confidentiality against the burden of keeping them secure. In addition, we will tend to keep the notes as brief as we can while still being as detailed as necessary to be useful.

With online counselling via email, though, the emails between counsellor and client are more than just notes: they are a verbatim transcript of the sessions. And, although our notes are (usually!) in plain script, we do not generally send them back and forth via theoretically open means of communication: to use the envelope analogy, most of us would think twice before even sending notes through the post in a *sealed* envelope, let alone an unsealed one.

So, clearly, some means of ensuring that our emails in transit are protected from prying eyes is important. Since we cannot practically secure the channel between counsellor and client's email in- and outboxes, we have to find a way of making sure the email is unreadable except by sender and recipient if we want to be confident of preserving the client's confidentiality.

As well as the security of messages in transit, though, we have another issue: who can read our emails in our inbox? If we are using our own PC, we have some control over that, as we can password-protect our account and make sure that nobody has access to our machine but us. In practice, that is more difficult, as many of us are sharing our PC with colleagues or family members, and if it is a machine at work, there is a good chance that our mail is stored on a server managed by an IT department. While they may have their own procedures for security, we cannot be sure that they, as non-counsellors, will subscribe to – or even be aware of – our standards in regard to confidentiality.

It should also be noted that the password protection used for things like email mailboxes has never been particularly strong, and they are a popular enough target for hacking types that there are quite a few tools out there for cracking the passwords that protect them. We cannot afford to assume that the security provided by default on our computers is adequate to protect sensitive client information.

What we therefore need is a way of ensuring that all messages to and from our clients are secure, whether they are travelling across the internet or sitting in our inbox or outbox on our PC. The solution to that problem is encryption.

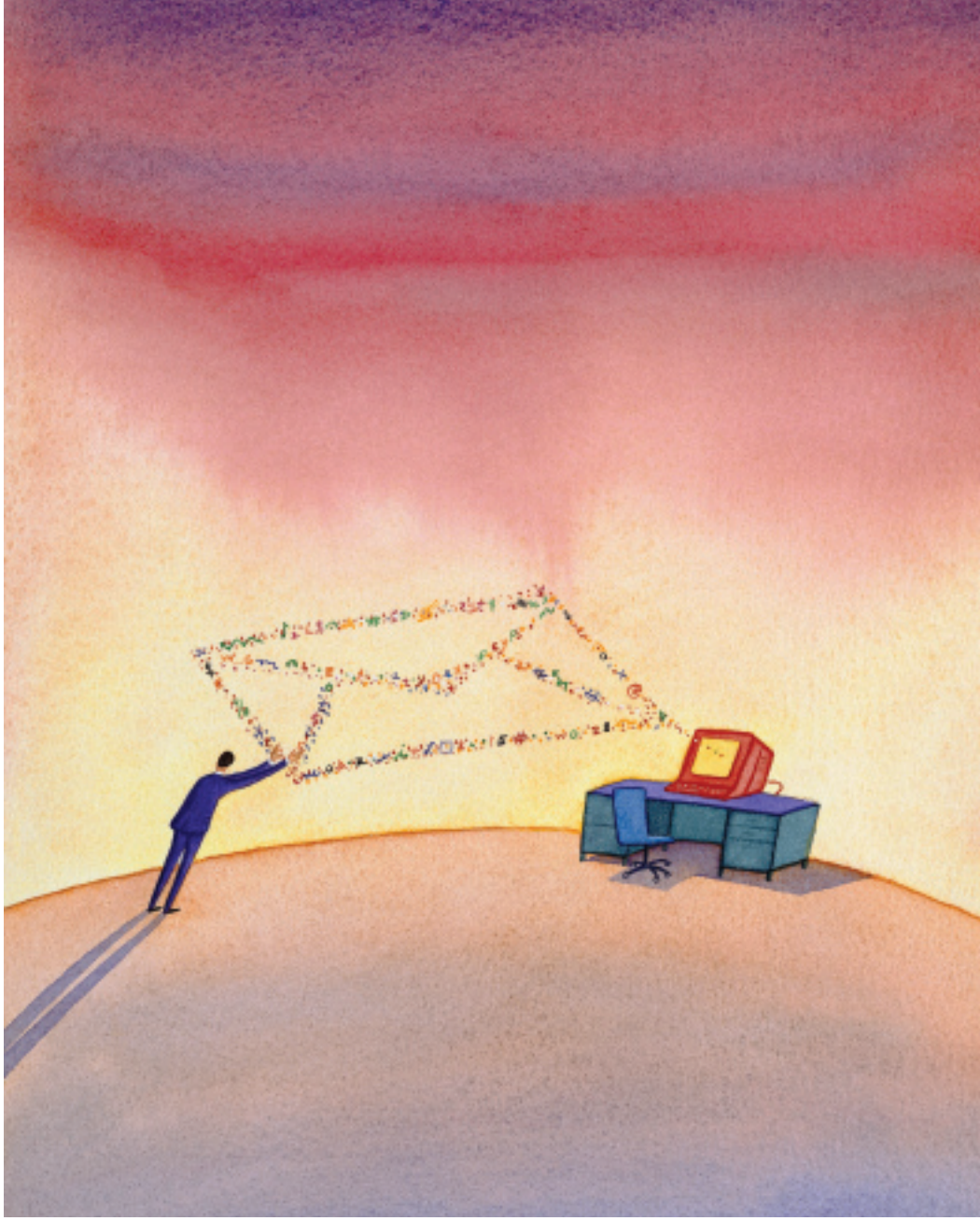
Encryption – a bit James Bond?

We tend to think of encryption as the stuff of spy novels: one-time pads, codes, ciphers, secret agents sitting in darkened rooms, and shortwave radios. In practice, it is far more mundane than that and we use it all the time: mobile phones use encryption to encode the digital representation of our voices, and online banking involves encryption to protect the traffic in transit, to name but two. Ciphers have been used since antiquity, with one of the simplest – an alphabetic substitution cipher – being named for Julius Caesar, who encrypted his messages to his commanders by shifting the alphabet along a number of letters. Such a system is trivially easy to break but represents the essence of what encryption is: a process of re-encoding the text of a message in such a way that only someone in possession of the 'key' to it can reverse the process and read the original text.

Nowadays, with computers, the encryption process can be far more complex, and the security of a particular method of encryption is generally determined by how long it would take for a computer to crack a given key. With strong versions of the encryption methods available to us today, that can be measured in years for an average desktop computer – more than adequate for our purposes.

In order to exchange encrypted messages we also have to exchange the key. The recipient needs a key to be able to decrypt a message we have encrypted, and we need to be able to decrypt theirs to us. Until quite recently this was a tricky problem but with the advent of another approach to encryption, called 'public key' cryptography, that situation has changed. Using public key encryption, we generate not one but two keys – a private key and a public one.

The public key can be freely distributed and can only be used to encrypt messages *to* us. It cannot be used to decrypt the message again, only our private key will do that. Similarly, our recipient also generates a pair of keys, and gives us their public one so that we can encrypt messages to them that can only be decrypted using their private key. And voila! We have a method of exchanging (and storing) emails that is as secure as it needs to be to preserve client confidentiality, both for messages in transit and when they end up in our inbox. The only item that is potentially vulnerable is our private key, which is password-protected but needs to be kept safe anyway. We will look at how that can be achieved shortly.



STOCKBYTE/GETTY

Sounds very complicated!

And with good reason: the whole point of encryption is that it is a complex process. Fortunately, we do not have to manage all of this ourselves. Most email clients, such as Outlook, support plugins that enable us to carry out the process of generating keys, encrypting and decrypting messages via menu options that protect us from the gory details.

As ever, there is a balance between ease of use and cost. Public key encryption software ranges in cost from completely free to around £100 – about the price of a cheap filing cabinet. What you get for your money varies. With the free solutions, you are on your own as far as installing and setting it up is concerned, and the integration with email software will not be as seamless, while the paid-for options give you a much more streamlined installation process, and complete integration with your email client. For non-technical users, the investment will be well worthwhile.

Drawbacks?

There are a number of additional things that need to be done when sending and receiving encrypted emails.

First of all, you will need to set up your private and public keys. This is not a terribly complex task and only needs to be done once but it might be daunting to

> Email is an insecure medium for confidential communications. The only practical way of ensuring security is to encrypt messages before they are sent, so that they are unreadable by anyone in transit over the internet

a very non-technical counsellor.

Then, you will have to encrypt your outgoing emails to your client(s), and decrypt their replies, which does add a slight overhead to the process, depending on whether you use an integrated (paid-for) plugin or one of the less streamlined free solutions.

Perhaps the biggest obstacle, though, is going to be getting your clients set up. For them to be able to read your encrypted emails (and encrypt their messages to you), they too will need to install encryption software. It may well be that clients are reluctant to spend money on an encryption plugin: that means getting them to use one of the free solutions, which they might find tricky to use. They will also need to install it on their computer and set up their keys, which may also be challenging to very non-technical users. The question of having a counsellor assist their client in setting up an encryption plugin raises some interesting boundary issues, too!

All these problems, to some degree, can be overcome and, once set up and underway, most people will have little difficulty doing the extra steps involved in encrypting and decrypting their emails.

Incidentally, for people using webmail services like Microsoft Hotmail, the importance of storing and transmitting the emails in encrypted form is even greater: those emails are effectively being stored on a public server to which anyone on the internet can theoretically gain access. Since most of us are quite lax when it comes to choosing secure passwords and keeping them safe, and given the possibility of breaches due to error at the server end, these systems are potentially very vulnerable.

There are also legal implications. If a therapist is ordered to disclose notes, they do always have the option to defy the court if they choose to (at some cost, in all likelihood). While the same would be true of emails stored on a computer belonging to the therapist, it would be legally feasible for a court to order a webmail provider to disclose emails on their systems. The therapist would therefore be denied some measure of control over this disclosure.

Of course, if the emails were encrypted this prevents the content being disclosed without the therapist's consent, but does still mean that a record exists that a conversation had taken place.

For these reasons, I would recommend that no therapist uses a webmail server to operate an email counselling service.

How does it work?

This depends on which software you are using to read your emails, and – to a lesser extent – on the encryption solution you choose. Broadly speaking, though, the steps will be: install the encryption software; generate your private and public keys; and provide a password to protect the private key. Once this is done, you are in business!

The same process will need to be carried out by each of your clients, too. Probably the best way to do this would be to arrange to have a supply of CDs for distribution to each client with all the software they need, and which they can install on their machine as simply as possible.

Encrypting your email with one of the streamlined solutions simply involves picking a menu option and typing in a password once you have written the message; the less comprehensive (but cheaper) solutions might involve you preparing your email in another editor (a word processor is very useful), copying the text into an encryption window, then pasting the encrypted message into your email client – this sounds rather more hideous than it actually is!

When you are receiving an encrypted email, a similar process but in reverse needs to take place: either you click a 'decrypt' option, type your password, and the plaintext message appears, or you need to do the copy-paste-decrypt thing again.

Your client will have to take exactly the same steps to encrypt and decrypt their emails.

Other basic precautions

Your private key needs to remain just that – private! Often, the best way to achieve this is to use a pen drive (many are now so small that they can hang off a key ring, which makes the 'key' metaphor almost literal), which plugs into a USB slot on your PC, but which you can take away with you when you leave the computer.

You can opt not to use a password to protect your private key but it is not recommended: it depends on how confident you feel that it will never fall into the wrong hands.

Conclusions

Email is an insecure medium for confidential communications. The only practical way of ensuring security is to encrypt messages before they are sent, so that they are unreadable by anyone in transit over the internet, or while they are stored in the mailboxes of the sender and recipient.

Public key encryption represents the best method for achieving this, and can be integrated into email clients with varying degrees of seamlessness.

To use encryption, both therapist and client will need to install suitable software onto their computers, which may present some technical challenges – the degree to which these are seen as show stoppers needs to be measured against the desirability of the use of encryption to maintain confidentiality.

If there is sufficient interest, I can evaluate a small number of encryption suites and write an article on the specific details of how to install and use them. ■

Stephen Allsopp is a college counsellor at Pembrokeshire College, Haverfordwest.
stephena@pembrokeshire.ac.uk