



Fee-Mail

A look at e-mail for solicitors practices

e-mail is a primary source of documentation for businesses and it has taken on an increasingly critical role in corporate litigation and court cases. Solicitors use e-mail as part and parcel of each case so it becomes critical even in non-contentious matters as it makes up part of the case history. Despite this, very few businesses, let alone solicitor's practices, have given any real thought to what this means. In this article we try to outline the main points to be aware of and how you can guard against falling foul of legislation, litigation or just bad business practice.

Time Is Money

Do you know how much of the e-mail you receive is junk? Junk or spam e-mail makes up an ever increasing percentage of mail that you receive and although statistics are hard to confirm (they tend to be out of date before they are published) it is estimated that anywhere between 40% and 80% of all e-mail is spam. All sorts of figures are bandied about but we do know that about 15 billion spam e-mails are sent every day so there is every chance some of it will come your way. As a "straw poll" we interrogated some of our client's systems to see how much spam mail they were getting over a 7 day period in July 2008. The table below shows the results paired down into differing practice sizes:-



Type of Practice	Mails Received	Number of SPAM mails	SPAM Percentage
1 Partner, 1 Office	408	208	51%
2 Partners, 1 Office	463	304	66%
3 Partners, 2 Offices	1,770	1,498	85%
10 Partners, 4 Offices	5,638	3,237	57%
Averages	2,070	1,312	63%

Assuming that a person takes an average of only 5 seconds to look at and then delete each spam e-mail this equates to a whopping 90 hours of lost time per year on the average figures shown above. Add to this the time taken to download all of this junk and the disk space taken to store it all, at least until it is deleted, and you can see how much of a problem spam e-mail has become.

Most modern e-mail clients offer some kind of junk mail filter but these are often inadequate with low detection rates and high “false positive” rates, where mail is flagged as spam when it is actually legitimate. Solicitor’s practices pose unique problems to anti-spam systems – for example, if most people receive a mail about mortgages it is going to be junk where someone is trying to sell them a mortgage deal (usually US based although, with the present problems over there, this is likely to tail off!). Solicitors, on the other hand, deal with mortgages day-in, day-out and a system that blocks mail on just a keyword basis would be infuriating as no mail about mortgages would ever get through. Junk e-mail filters such as the one in Microsoft Outlook work on keyword lists and known spam definitions and, although a step in the right direction, they can never catch all junk mail.

Luckily, help is at hand. There are a number of anti-spam systems which can dramatically reduce the amount of junk e-mail your personnel have to deal with. The best ones are centrally based, checking e-mail as it comes into your practice and before it is forwarded to the final recipient, which means there is only one system to keep up to date. They also use a variety of techniques to spot spam e-mail including key word checking, DNS Blacklist checking, Sender Blocklists and Bayesian Analysis. Using multiple methods of detection catches more spam and reduces the number of false positives. The very best of the best can catch around 98% of spam e-mail before it hits your inbox.

Don’t Blame Me

There is no legal authority on the effectiveness of e-mail disclaimers but that is not to say that they should not be used, provided care is taken in drafting them. Similarly, confidentiality notices may be used at the foot of e-mails to safeguard, as best one can, against the e-mail going astray.



In addition, if your practice is a Limited Liability Partnership then there is certain mandatory information that should appear on every e-mail you send:-

- Your company registration number;
- Your place of registration (e.g. Scotland or England & Wales); and
- Your registered office address

If you are using stand-alone e-mail software then you will need to add your disclaimers, confidentiality notices and mandatory information to each PC’s e-mail software. However, if you are using a centralised e-mail system such as Microsoft Exchange or Lotus Notes then you can install software that automatically adds these items to all e-mail that is sent out.

Finally, if you are really serious about securing your e-mail then you should consider an e-mail encryption system. These systems “scramble” your e-mail so that it is unreadable by anyone other than those with the correct key so even if an e-mail does go astray you can be safe in the knowledge that no one else can read it.

Safe Content

e-mail is a powerful tool but it is open to abuse. Most viruses come into a PC via e-mail because it is so easy to attach unwanted items to something which is used by practically everyone. Catchy and intriguing titles persuade many to open e-mails that contain potentially hazardous programs which can lay waste to your computer or inundate you with unwanted messages and pop-ups.



As responsible lawyers you will all have up-to-date anti-virus protection on your PCs and servers but it is better to eliminate viruses at the source rather than to wait until they hit a user's inbox before removing them. To this end a number of e-mail scanning solutions are available which remove viruses, Trojans and phishing attempts before the e-mail ever gets near to the end user. As long as you pick up your e-mail at a single source (e.g. Microsoft Exchange Server, Lotus or Domino Server or other SMTP or POP3 server) you can apply one of these solutions to ensure that all e-mail messages are scanned and cleaned before they come in, or even worse leave, your offices.

The other problem with e-mail is, of course, that anyone can write anything and send it to anyone else. Content management of e-mail is becoming increasingly important for all businesses as laws governing what is and is not acceptable behaviour change with an ever increasing frequency.

There are opposing laws that say whether you can or cannot monitor the e-mails being sent by your employees (specifically Regulation of Investigatory Powers Act 2000 [RIPA] and the Data Protection Act 1998 [DPA]) but the general consensus seems to be that only "light" monitoring is the best way forwards. So how do you know if e-mail being sent by your firm has unwanted, or even illegal, content? The straight answer is that you don't and you may not be allowed to find out. However, you could well be liable if one of your employees is sending e-mail containing unwanted material.

The way around this is to implement an automatic content management system which "vets" e-mail being sent and quarantines suspect e-mail for the attention of a supervisor. Using this kind of system no real "monitoring" is taking place so you cannot fall foul of the privacy legislation but you can sleep easy knowing that e-mails with unwanted content are being weeded out before they leave your offices.

Marketing

As we have said, e-mail can be used to send anything to anyone. This makes it a powerful marketing tool and you can use it to send newsletters, law updates or whatever else you think your client base would be interested in.



If you are sending to a handful of people you can use your normal e-mail software but addressing each person by name at the top of the e-mail will make it seem more personal and may get a better response. Using normal e-mail software you would either have to send each mail individually or you can get some add-ons that do this job for you.

A much better approach, especially if you are sending to more than a few dozen people, is to employ the help of an e-mail list service. These services provide facilities to personalise mass e-mails as well as maintaining the recipient list allowing subscriptions, un-subscriptions and automatic removal of “bounced” e-mail addresses.

Who Said That? (and how do we prove it?)

Many practices have no idea where their e-mail is being stored. Even in firms where central mail servers are employed, e-mail may be scattered to the four winds once it gets “archived” off the main mail server. The usual process with, say, Microsoft Exchange Server is that mail is kept on the mail server for a certain period then it is “auto-archived” off to a PST file on the user’s PC. Thus, each PC contains some e-mail history but there is no central place where you can find a missing mail or that important piece of evidence.



Even without the importance given to e-mail as part of a case history, there are some statutory reasons for looking after your e-mail:-

- The Data Protection Act 1998 - The DPA says that individuals have a right to obtain a copy of personal data held about them. The Data Protection Registrar has recently been targeting solicitor’s practices for non-compliance so you need to be registered and to be able to easily retrieve any e-mail pertaining to your clients.
- Disclosure - During court proceedings disclosure orders require parties to make reasonable searches for data and this is now extended to deleted documents and those on your backups. Once again you may need to rapidly find all e-mail quickly and efficiently.
- Freedom of Information Act - If you work for public bodies you might be caught by this one too. This Act gives the public rights of access to recorded information such as e-mails. Information must be provided if it is at all recoverable (e.g. any trace of it exists on your computers).

It isn’t really good enough to store mail in an ad-hoc and haphazard manner. You need a central mail retention policy and a means of storing all e-mail, either inbound or outbound, in a single, searchable store. Only then can you comply with the various pieces of legislation covering e-mail retention and have any hope of pulling back that all-important lost e-mail.

Simply put, there are two options: keep everything or delete everything. Keeping everything is the best option because e-mail is a two-way communication process. Deleting an e-mail does not erase all traces of that communication because at least one recipient would also have a copy. Keeping a copy of every e-mail will ensure that your own e-mail will not be used against you. Practices also need to define a retention policy based on the importance of the e-mail being archived. The Senior Partner's e-mail, for example, should be retained for longer periods than that of an office junior.

Using a central e-mail archiving system all e-mail is stored in a central location and is easily accessible by end-users using a web browser or similar access method. In addition, by using the auditing functionality, practice management can access any e-mail that is requested for e-discovery or e-mail compliance purposes and guarantee that these e-mails have not been tampered with.

Mail on the Move

You've probably all heard of the Blackberry device and some of you may even have them already. For those of you still in the dark, a Blackberry is like a clever mobile phone that also receives your e-mail wherever you are.



The downside of the Blackberry is that it is quite bulky and requires an investment in infrastructure at your offices and in the phones to make the e-mail system work. All well and good for those of you with Blackberry mail servers already installed but there are alternatives.

If you have a Blackberry device but no infrastructure to support it then some mobile phone companies provide a simple Blackberry account which allows you to receive your e-mail. It normally requires either a Microsoft Exchange Server account somewhere (maybe your office, maybe on a hosted system) but then reads mail from this account and "pushes" it out to your Blackberry device. These systems are great for small numbers of Blackberry devices but can get complex if you try to manage too many phones this way.

Failing that, Microsoft's Exchange Server supports push e-mail now so you don't have to rely on a Blackberry to receive your mail on the move. This system can send mail to any mail-enabled mobile device although devices running Windows Mobile v5 or v6 are the preferred option. Lots of smart-phones and PDAs now run systems capable of receiving push e-mail so you are no longer tied to a Blackberry.

Finally, if you have a POP3 mail account, and most mail systems offer this, you can setup your mobile phone to send and receive e-mail. Pretty well all mobile phones these days offer this feature and it is just a matter of setting the thing up properly.

In summary, there really isn't any reason why you can't receive mail on the move – unless you just don't want to!

Sales Alert!

If nothing in this article interested you at all you can skip this section entirely. If, however, there was something that might fit with your practice then read on...



Professional Technology has been supplying e-mail management systems for a number of years. We are constantly on the look-out for systems that are easy to use and, most importantly, easy to manage because we know that solicitors are not necessarily the most IT literate people in the world.

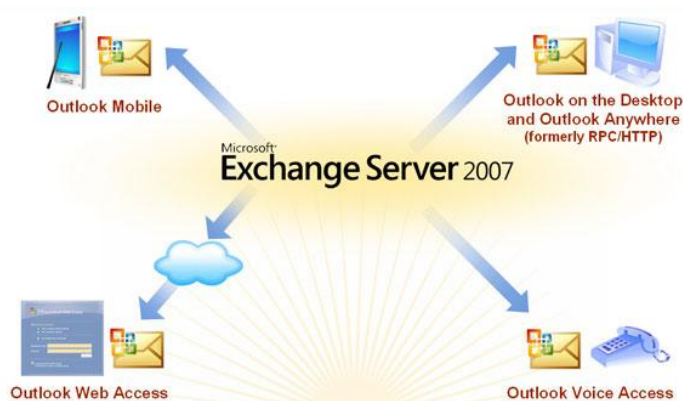
We have put together a package of systems which we consider to be the best in their field to cover all of the main points raised in this article. These systems are in use in thousands of businesses world-wide and in many of our clients throughout the UK so we know they work which is always a good thing. We also use them here at PT of course!

Mail Server and Mobile e-mail

Microsoft Exchange Server

e-mail is the mission-critical communications tool that allows your personnel to produce the best results. This greater reliance on e-mail has increased the number of messages sent and received, the variety of work getting done, and even the speed of business itself. Amid this change, employee expectations have also evolved. Today, employees look for rich, efficient access to e-mail, calendars, attachments, contacts, and more no matter where they are or what type of device they are using.

Microsoft Exchange Server 2007 has been designed specifically to meet these challenges. The new capabilities of Microsoft Exchange Server 2007 deliver the advanced protection your practice demands, the anywhere access your personnel want, and the operational efficiency you need. Exchange Server allows access to your e-mail via a rich client, such as Microsoft Outlook, a web browser or from your mobile device and can deliver mail wherever you are in the world.

*Spam, Disclaimers and List Server*

GFI MailEssentials

The problem of spam e-mail is countered by the excellent MailEssentials system from GFI Software. With over 60 awards to its name, 80,000 satisfied customers and the lowest prices on the market, GFI MailEssentials is an anti-spam filter that captures over 98% of spam and, since it is server-based, it eliminates the need to install and update anti-spam software on each desktop.

GFI MailEssentials also enables you to add disclaimers to the top or bottom of an e-mail. Text and HTML formats are supported. You can include fields/variables to personalize the disclaimer. You can also create multiple disclaimers and associate them with a user, group or domain.

MailEssentials also includes a list server service so you can use it to send newsletters and other bulk e-mails to your clients on a regular basis.

Content Management and Security

Content management and security is dealt with by MailSecurity also from GFI Software. Complementing the MailEssentials product or running on its own this system provides not one, but up to five anti-virus engines running on the e-mail server. With multiple anti-virus engines you:-

- Reduce the average time to obtain virus signatures which combat the latest threats
- Take advantage of all their strengths because no single AV scanner is the best
- Virtually eliminate the chances of an infection
- Get a product that is cheaper than any single AV engine solution.

With over 30,000 customers and the best price on the market, GFI MailSecurity acts as an e-mail firewall protecting you from e-mail viruses, exploits and threats, as well as e-mail attacks targeted at your organization.

Mail Archiving

Making up the trio of GFI products is MailArchiver. GFI MailArchiver, is an e-mail archiving and e-mail management software package for Exchange Server. With over 10,000 customers, GFI MailArchiver is the no.1 e-mail archiving software for small and medium sized businesses and it is used by administrators to maintain a copy of all corporate e-mail correspondence, manage and reduce the company's dependency on PST files and also meet a growing number of regulations on compliance, eDiscovery and other legislation. Furthermore, this easy to install product requires very little administrative effort and most importantly ships at the lowest price on the market.

Professional Technology (UK) Ltd

375 High Street
Rochester DX: 6508
Kent, ME1 1DA Rochester

Phone: 01634 815517
Fax: 01634 829032
Email: sales@ptuk.co.uk
Web Site: www.ptuk.co.uk

If you would like any further information on this topic please contact us at the address to the left or visit our web site www.ptuk.co.uk.

©. Professional Technology. The Author asserts its right to be associated with this work. The information contained in this document is commercially sensitive to the author. It is intended only for the information of the addressee(s). This document may not be distributed or disseminated in any way to any third party without the express written consent of the authors.