

How to protect your company's e-mails from prying eyes

One of the most important aspect of communication should be confidentiality, that is especially true when you are a lawyer or a notary and you need to deal with your customer's privacy. As you should know sending an e-mail is like sending a postcard, therefore confidentiality is lost by the very nature of e-mail communication. That is because your e-mail are hopping from outgoing mail servers to switches and networks, then reaching other isp incoming mail servers and god forbid if unencrypted wireless access points were not used along the links. Anywhere along these hops can anyone equipped with freely available sniffer tools get access to any unencrypted private data. Scarry, isn't it? Hopefully there are many easy to apply solutions that allows you to get the full benefits of e-mail without the disadvantages.

When we say easy, we mean that many web hosting providers can already provide good privacy for very little since most of the good tools that have been around for over a decade now are based on know-how. This is therefore an educational issue. Let me illustrate with two simple solutions based on some of the most common situations: I think that the best solutions are the simplest and that anyone SHOULD at least have the following first point as a standard policy, even if you think privacy is NOT an issue for you. Cases: 1. When accessing the Internet via an open wireless network, you need to make sure that your e-mail access are going through a secure protocol (or a tunnel) such as SSL; all mail clients such as outlook express provide that capability. 2. You must assure confidentiality to all your customers, the cases of clients of most notaries and lawyers, but also for software developers and the like when source code is updated or transferred. Solutions: In the first case, this is extremely easy by using a ssl encrypted mail servers and this should be the default for any serious office, ask you isp or switch to an isp who will spend the time to help you set it up. In the second case, what you can do is to provide free e-mail addresses based on your domain to all customers who have accounts with your firm and instruct them to simply use your ssl encryption to send/receive e-mails to your agents. This is very good for lawyers and notaries as this is in fact creating an extranet (which is like an intranet but accessed from the outside) and there is no unencrypted communication to any other servers than the one where your domain is hosted. In addition when you need even higher security, you can have your own private and dedicated virtual mail server outsourced BUT only accessible by your trustworthy network administrator who can access and maintain it. If you are paranoid you can even encrypt the mailbox content on the server itself or even the whole disk partition. This is usually much more expensive but only you know how much value the information is worth. Now that you know, should you ask me why you should go to the trouble of setting up such account? I would answer: I have not been presented with any evidence or proof that the knowledge and the providers were not available to assure your company's privacy. When you want my help on that, simply [click here](#) .