



## Security and your website

One of the biggest issues I come across as an ISP & web developer is the lack of knowledge regarding security on the Internet and what should be done and whose responsibility it is.

### SSL certificates

When shopping online and entering your credit card information, you should ensure as a user that the site has a padlock in the bottom right of the browser and that the padlock is valid. (You can double click the padlock and if there is a problem with it there will be an error). You should ensure that any website you have had developed has its credit card page hosted on your ISP's secure certificate. However simply having this doesn't make your website secure, or the users information safe.

### Credit card data

What's then done with the credit card data is key to security, I have come across sites far too often that hold the credit card numbers of all past orders in a database on the web server with no security at all, leaving it open to abuse by hackers or even an unscrupulous ISP! The other thing that can happen is that after been collected the credit card information is simply emailed to the company. The content of these emails can be 'sniffed' by hacking software to read what's in them.

If credit card details must be stored on a web server, which to be honest, they really shouldn't be stored for any length of time at all, then they must be encrypted. If credit card details are emailed, then they too must be encrypted before being sent. There are many products that can encrypt data, PGP and S/MIME are two of the large ones, and these can be used to encrypt both your emails and the rest of your computer files.

Since there are no authorities to regulate ISP's or web design companies, it's up to you to ensure that your website is safe for your customers to use. Always check the SSL certificate and ask your developer about what happens to the credit card data and if it is encrypted.