Some of the principal barriers which impede the full development of e-business are the lack of trust and the sensation of insecurity. There are two aspects which must be taken into consideration with regards to Internet security: applications which contribute to an efficient control of access and to the management of the users and the computer systems (hardware and software) which make up the architecture necessary for network connections.

Whenever a novice user wishes to access any additional service offered by a web page, such as newsletters, there is usually a prior data request. This creates a sensation of mistrust which may stop him from proceeding. This policy, which the majority of Internet companies apply, is a requirement which is closely related to the nature of secure online business. In order to have control over users and so avoid unwanted intromissions, the use of an authentication source is indispensable. There are currently two mechanisms used by more than eighty percent of Internet Web pages: the so-called cookies, a kind of online identification document which each server issues and which is sent to the user’s computer in order to identify him when he returns. The second mechanism is the authentication by granting each user a name and password and by obliging him to first register his details.

Alternatives
These mechanisms, although very widely used, are insufficient as a means to offer secure identification of the user and to ensure his privacy. Over the next few years, it is envisaged that there will be a significant growth of new systems which provide more security, such as digital certificates, smart cards or biometry systems which identify the Internet user by way of his fingerprint or the iris of his eye. Taking into account that the Internet is a network of other networks, it is obvious that a variety of means of intromission in these networks have emerged, the only aim of which is to challenge the security of the systems which make up the computer architecture and to make use of the valuable information stored there. One of these intromission routes is through the web servers, which, although they are protected by firewalls, may be violated depending on their level of sophistication. By attacking the web servers, one can obtain all the information necessary in order to hack the system and render it temporarily inoperative or gain access to confidential files.

It is obvious that the usefulness of the Internet, which interconnects servers in order to share authorised information amongst those users who so wish, has turned into a large threat to all companies operating on the net. For this reason, it is logical that there appear cases of companies affected by attacks upon their web servers, either by hackers or by a virus.
One of the intrussion routes which affects security comes about through the interception of privileged data and information at the moment they are sent from the user's browser or vice versa. It is in this type of intrusion that economic fraud takes place.

There are more and more routes and ways which bring privacy and security on the net into question. This creates mistrust in the user and means that only a small proportion of the Spanish population connected to the Internet carry out purchases.

According to a recent study, 68 percent of Spanish Internet users believe that security is an obstacle which impedes the development of online business. For this reason, more and more companies are becoming aware of the importance of security in their systems, even though the budgets assigned in this regard are still meagre. Forrester Research affirms that in 2002 companies will spend 55 percent more than what they spent in 2000, and forty percent of the total will be destined to software products in order to strengthen security. Moreover, it is believed that the outsourcing of security which the majority of firms opt for will see a downturn in 2002 and begin to recover in 2004.

Despite the deficiencies in security, one cannot demand that a recently created channel, which is still immature, be able to offer perfect security which has never been achieved in the traditional economy.

**The Question**

"How should entrepreneurs invest in order to achieve user security and confidence?"

**Inmaculada Fernández Gallardo, Technology Manager, PricewaterhouseCoopers**

A critical factor in making the Internet a solid environment in which to carry out business is the existence of trust between the participators in the transactions carried out over the same. Here we refer not only to the trust which the two parties in the operation (for example, client and bank) deposit, but also the trust of all the agents who directly or indirectly intervene in this activity. If we understand security in Internet commercial activity as being the protection of confidentiality, integrity and the availability of the information necessary to carry out this activity, it is important to emphasise that security is fundamental in order to achieve the aforementioned trust. But the focus which is most commonly applied is that of converting the issue into something which is exclusively technology-based. Whilst it is true that in security there are complex technological aspects, the indispensable starting point is an appropriate level of awareness about this issue by the agents intervening in the commercial transactions over the Internet and, in general, by the public.

**Brian Subirana, IESE Professor**

There are three areas in which companies may intervene. Firstly, by informing of the policy followed by the company. In many cases, companies do not clearly indicate the use which will be made of information collected over the Internet. This does not refer only to information relating to the means of payment used, but also to personal information such as the activities carried out within the service. Secondly, new methods which impede the use of the data stored by the company need to be developed. Instead of centring payment on systems based on traditional credit cards, other mechanisms
which impede fraud need to be promoted. Finally, there needs to be development of a support industry for the means of payment and security systems in which digital notaries public, certifiers, online regulating agencies, insurance agencies and banks all intervene. Hence, clear information, alternative payment methods and the support industry will contribute to the development of trust on the net.