

Payment cards: Safety on the internet

When shopping or performing transactions on the Internet, usually the following data are requested:

- Name and surname of the credit card holder
- Card expiration date
- Card identification number (CIN) or card security number, usually located on the back of the credit card.

When you enter your credit card details or other personal information, make sure you are using an **encrypted** website (you can easily identify it because the URL address at the top of your computer screen will start with the letter "https" when you are on a secure page). The process of encryption prevents unauthorized individuals or hackers viewing your information as it is securely transmitted over the Internet.

To minimize the risk of credit card fraud first of all make sure you don't let your card out of sight when making a transaction. Secondly, when using the Internet make sure you are shopping at a secure and trustworthy website, choosing from reputable stores and sellers:

- Make sure the website you are using has security protocols allowing user identification. Secure Socket Layer (SSL) is the most common tool used for secure network communication: usually, when performing a transaction, a closed padlock icon appears on the bottom right of the browser window, meaning that the connection is secure.
- The use of internet banking is recommended as it offers you the possibility to check your statement almost in real time, so that you can contact your financial institution immediately in case you notice any fraudulent activity on your account.

Check your statements carefully. If you find any unfamiliar transactions contact your bank or building society immediately.

16/03/2011