Polizia di Stato

How to protect our credit card

One of the typical systems used by con men to capture both PIN and credit card data is called skimming. It consists in stealing magnetic stripe data by simply swiping the credt card through a device called a "skimmer".

The skimmer can be no bigger than a pack of cigarettes and powered by battery. But it can be even larger and store up to several dozens of magnetic stripes.

Unlawfully intercepted data are transcribed on a plastic support, with the features of a credit/cash card, through a common PC and a software for the management of magnetic stripes.

The skimmer, of course, is a device different from the normal P.O.S. orivuded by issuing company.

To run this kind of scam, the con man must take possession of the customer's credit card for a few seconds, out of his/her sight.

Here there is a list of things that a credit card user should do to reduce the possibility of card cloning and skimming:

1. Do not give your card to any other person.

2. Never lose sight of your card when making a payment.

3. Be wary of any commercial enterprise that claims to have no P.O.S. terminal close to the cashier.

4. When you receive your credit card and PIN code, check that the envelope is intact, that it is from your bank, your credit card issuer or the company in charge of postal delivery services.

27/04/2011