Bancomat clonato: che cosa fare?

Come verificare di essere stati clonati
È piuttosto difficile accorgersi di essere stati clonati al momento in cui si va prelevare.

Normalmente le operazioni eseguite con il bancomat si fanno meccanicamente e di fretta.

Ma poi ... Poi possono succedere due cose. Eseguite un estratto conto di routine e vi trovate con dei prelevamenti che non avete fatto. Oppure venite informati dalla vostra banca che il vostro bancomat è stato scoperto fra altri clonati dalle forze dell'ordine dal sistema bancario che hanno verificato che il vostro bancomat è stato utilizzato da una apparecchiatura che poi si è verificato essere stata clonata.

Oddio mi hanno clonato !
Innanzitutto "no panic". Oramai le banche si sono arrese a rimborsare tutti i correntisti che hanno subito la clonazione della carta e che sono ovviamente in grado di dimostrare la loro buona fede e le transazioni fraudolente.

La procedura è abbastanza semplice.
Bloccate subito il vostro bancomat attraverso la vostra banca o meglio attraverso il numero verde.

In questo modo il vostro bancomat, e quello clonato, diventano inservibili.
Passate dalla vostra banca oppure attraverso il vostro internet banking ricavatevi una lista delle operazioni fraudolente con data, ora della transazione, importo e se possibile il luogo dove è stata effettuata.

Unione *dei* Comuni
TERRE dell'OLIO e del SAGRANTINO

Prendete il vostro bancomat, che in effetti oramai non serve a nulla dal punto di vista bancario, ma vi serve per dimostrare che non lo avete smarrito e che lo avete usato e detenuto correttamente.

Presentate quindi denuncia presso il posto di Polizia, o Carabinieri o altre forze dell'ordine.

La denuncia riguarda la clonazione della carta e le operazioni non eseguite.
Con la vostra denuncia presentatevi nuovamente alla vostra banca dove presumibilmente compilerete dei moduli che istruiranno la pratica per il vostro rimborso.
I tempi del rimborso variano da banca a banca e da burocrazia a burocrazia.

...In ogni caso di dubbio o sospetto, chiamate subito il

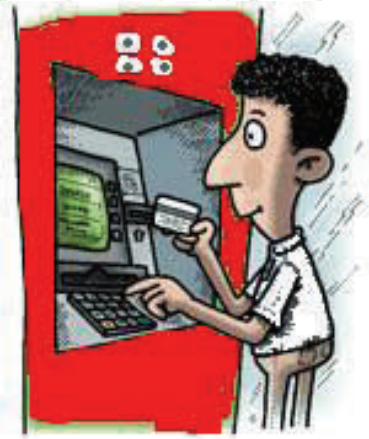
112

Realizzato da Francesco Caccetta

Unione *dei* Comuni
TERRE dell'OLIO e del SAGRANTINO

Clonazione bancomat:

come difendersi



Alcuni consigli.
Se possedete un Bancomat:

1. Estratto conto: controllatelo con attenzione ogni mese, poiché è l'unico modo per accorgersi di eventuali spese mai effettuate. Molto utile a questo scopo la possibilità di Internet banking offerta dalla vostra banca, che vi permette un controllo anche giornaliero sul vostro conto.

2. Allo sportello, osservare l'apparecchiatura di fronte a voi alla ricerca di anomalie o stranezze. Sulla verticale o diagonale della tastiera può esserci per esempio una microtelecamera.

3. Bocca della fessura: controllate se la fessura dove si inserisce la tessera bancomat è ben fissa. Se si muove o si stacca potrebbe significare che è stata coperta con uno *skimmer*.

4. Tastiera: verificare se anche la tastiera è ben fissa. Spesso i malfattori sovrappongono una loro tastiera fittizia per catturare il codice PIN. In questo caso c'è un gradino di un paio di millimetri.

5. Codice PIN: digitate il codice nascondendo con il palmo dell'altra mano l'operazione. Nel caso sorgano in voi dei dubbi, non introducete la tessera e non inserire il PIN. Se la manomissione dell'apparecchiatura è evidente chiamate le forze dell'ordine.

6. Se il Bancomat trattiene la vostra tessera e qualcuno si avvicina dicendovi che anche a lui è appena successo la stessa cosa e vi invita a digitare di nuovo il PIN per sbloccare la carta, diffidate e non fatelo! In ogni caso di dubbio o sospetto, chiamate subito il 112 e riferite i fatti per evitare che qualcun altro ci cada.

qualche semplice buona idea per ridurre il rischio di furto o clonazione di bancomat e carte di credito:

1. Mai tenere il codice PIN e la carta insieme, nel portafoglio o nella borsetta, ma custodirli separatamente, meglio ancora memorizzare il codice. Sembra incredibile, ma c'è ancora chi per ingenua comodità scrive il PIN sulla carta bancomat o di credito o sull'apposita custodia.

2. Per quanto riguarda le carte di credito, prestare sempre molta cautela nel lasciare i dati per eventuali transazioni via Internet. Come regola molto generale, fidarsi solo di aziende/negozi noti.

3. Fare attenzione in bar o ristoranti a consegnare la carta di credito a persone che non si conoscono: meglio piuttosto consegnare la carta direttamente alla cassa e averla sempre sott'occhio. Non permettere a camerieri o cassieri di allontanarsi con la nostra carta.

4. Attenzione alle moderne truffe con il bancomat: se la carta si inceppa nell'apparecchio di prelievo, non abbandonate per nessun motivo lo sportello, fino a quando non siete riusciti a comunicare alla banca il blocco. Molti casi i truffatori simulano questo genere di "incidenti".

5. Quando vi viene recapitata a casa, per posta, la nuova carta di credito o il bancomat e il successivo codice PIN, controllate che le buste siano integre e che siano della vostra banca (o di chi emette la carta di credito). Verificate che all'interno non vi siano alterazioni o rotture del cartoncino che contiene la carta.

Non cedete mai la vostra carta e il vostro PIN ad altre persone.

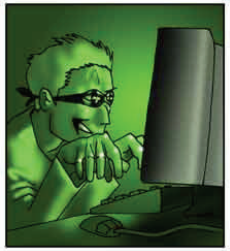
...per i possessori di carta di credito:

1. Estratto conto: controllatelo con attenzione ogni mese, poiché è l'unico modo per accorgersi di eventuali spese mai effettuate. Molto utile a questo scopo la possibilità di Internet banking offerta dalla vostra banca, che vi permette un controllo anche giornaliero sul vostro conto.

2. La tessera: non perdetela mai di vista.

3. Internet: nel caso di acquisti sul web, verificate che la pagina del sito in questione sia sicura (che usi cioè algoritmi di *crittografia*, contrassegnata da un lucchetto posto sulla parte inferiore destra della finestra). Se così non è, diffidate e non comprate nulla: non avete a che fare con persone serie.

4. E-mail: se vi arrivano messaggi di posta elettronica dove vi si chiedono dati sensibili relativi alla vostra carta di credito o al conto corrente, non rispondete a nessuna richiesta! Si tratta di *phishing*, una truffa.



Unione *dei* Comuni
TERRE dell'OLIO e
del SAGRANTINO