Questura di Firenze

Come difendersi dalla clonazione?

Guida per l'utente

In collaborazione con

Bassilichi

Premessa

- L’utilizzo di carte bancomat e di credito è ormai molto diffuso, ma con la diffusione aumentano i rischi a carico degli utenti.

Sai davvero tutto sul Bancomat?

- “**Bancomat**” è il nome con cui vengono chiamati in Italia e in molti paesi europei gli sportelli automatici per il prelievo di denaro contante dal proprio conto corrente bancario, attraverso dei distributori collegati in rete telematica, anche fuori dagli orari di sportello ed in località diverse dalla sede della banca presso cui si intrattiene il conto.

- Nei paesi di lingua anglosassone il sistema è noto con la denominazione generica di ***Automated Teller Machine*** **(ATM).**

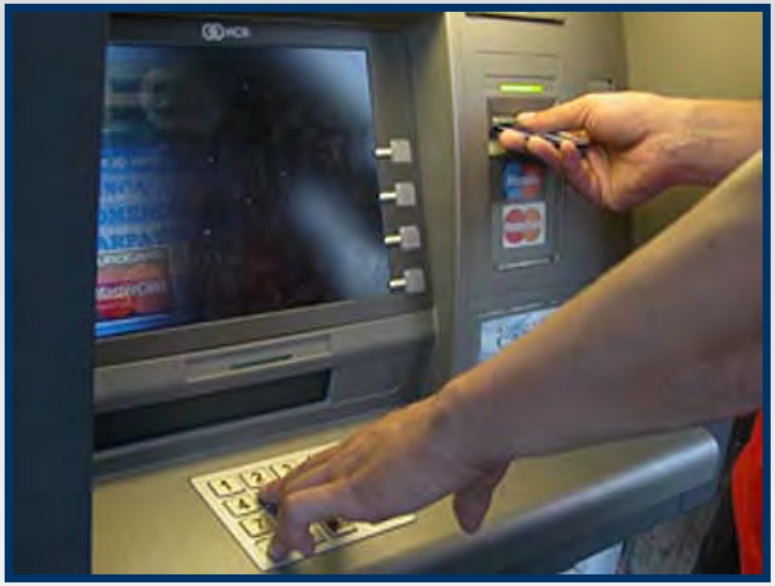
Sai davvero tutto sul Bancomat?

- Il servizio Bancomat è fornito dalla maggior parte degli istituti bancari ed ha costi e modalità di funzionamento variabili a seconda delle condizioni stabilite tra la banca ed il cliente. In generale, le apparecchiature possono appartenere anche a una banca diversa da quella presso cui il cliente ha il conto.

- Con il servizio Bancomat è possibile effettuare altre operazioni oltre al prelievo, quali il pagamento di bollette, il versamento di contanti e assegni, la lettura del saldo, la stampa degli estratti conto o della lista dei movimenti e le ricariche dei cellulari.

Come funziona la carta?

- Per l'identificazione dell'utente il sistema sfrutta una tessera plastificata (**badge**) corredata di una **banda magnetica** e, solo in quelle più moderne, anche di un **microchip**.



- Dopo che il cliente ha inserito la carta nel lettore, questa viene attivata digitando sulla tastiera un **codice numerico** (**PIN**), che deve essere mantenuto segreto dal possessore.
  Il PIN, per ragioni di sicurezza, viene criptato, cioè inviato ai canali bancari sotto forma di codice alfanumerico.

Come funziona la carta?

- Se la stringa criptata corrisponde a quella memorizzata o ricalcolata sul calcolatore centrale, l'operazione può essere eseguita.

- La carta può anche essere utilizzata per effettuare pagamenti negli esercizi commerciali provvisti di un piccolo dispositivo che tecnicamente si chiama **Point of Sale (POS).**

La clonazione… come agiscono i malviventi?

- Per clonare una carta è <u>necessario entrare in possesso di due dati</u>:
  - **CODICE DELLA BANDA MAGNETICA**
  - **PIN**

- Solo la disponibilità di questi due elementi **<u>consente di ricostruire (clonare) una scheda magnetica</u>**.

  I dati acquisiti con la frode possono essere copiati direttamente sulla banda magnetica della carta falsificata oppure rivenduti a criminali che si occupano della successiva codifica.

  Una carta falsificata sarà utilizzata per effettuare prelievi e altre operazioni sino a che l'utente o il sistema antifrodi del circuito bancario non provvedano alla sua disabilitazione.

La clonazione… come agiscono i malviventi?

1 Skimmer

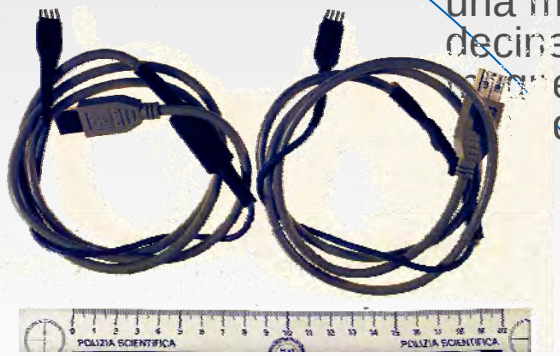
Si tratta di un dispositivo che **cattura i codici contenuti nella banda magnetica con la semplice "strisciata" della carta bancomat o di credito**.

La clonazione… come agiscono i malviventi?

1 Caratteristiche dello Skimmer

- non ha una forma standard: può essere piccolo quanto un pacchetto di sigarette oppure di dimensioni più grandi;

- può essere auto-alimentato con batteria;



- può arrivare ad immagazzinare, tramite una memoria eprom, diverse decine di bande magnetiche (i dati di oltre 200 di credito);
- viene collegato a un PC, munito di un programma di gestione per bande magnetiche, con il quale si trascrivono i dati, presi illecitamente, su una carta vergine con le caratteristiche di una carta di credito/bancomat.

Di solito viene montato nella fessura di inserimento della carta sulla parte frontale dello sportello bancomat. Nel caso di utilizzo di carta di credito in esercizi commerciali, la carta viene passata prima nel terminale P.O.S. e successivamente nello skimmer.

La clonazione… come agiscono i malviventi?

2 Lebanese Loop (cd. "*lingua di coccodrillo*")

Sullo sportello di prelievo automatico viene applicato un ***dispositivo che trattiene la carta*** in modo che non venga più restituita.

A questo punto può intervenire il truffatore che, fingendo di prestare soccorso al cliente davanti allo sportello, lo invita a digitare nuovamente il PIN consentendogli così di vederlo e memorizzarlo.

Dopo l'allontanamento della vittima, il criminale può recuperare la carta e utilizzarla con il PIN appena memorizzato.

La clonazione… come agiscono i malviventi?

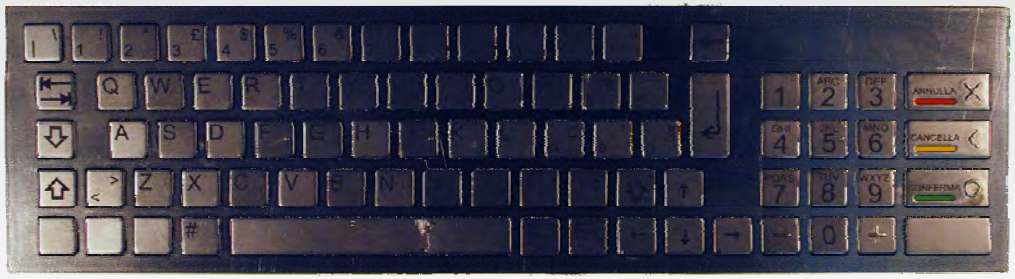
3 Mini telecamera

Per entrare in possesso del PIN della carta, i malviventi installano a volte una minitelecamera sulla parte frontale dello sportello automatico, spesso accanto alla plafoniera della luce o nella fessura per l'introduzione di auricolari per non vedenti.

La clonazione… come agiscono i malviventi?

4 Tastiere finte

I malviventi riescono a manomettere lo sportello apponendo una falsa tastiera, identica come dimensioni e caratteristiche a quella reale.



La clonazione… come agiscono i malviventi?

5 Manomissione del POS

Il P.O.S. utilizzato negli esercizi commerciali viene aperto e all'interno viene istallato un microprocessore che registra i codici della carta di credito o il PIN.

Il microprocessore viene, poi, rimosso ed utilizzato dal criminale per ricreare nuove carte di credito grazie ai dati immagazzinati.

La clonazione… come agiscono i malviventi?

6 Trashing

I truffatori utilizzano gli scontrini delle carte di credito che talvolta gli utenti gettano via incautamente dopo un acquisto.

UBI BANCA

N.RO SPORTELLO AUTOMATICO 0600
DATA 31/12/07 ORA 15:20
N.CARTA 00000254 N.TRANS. 184

TAGLIO	COMMISSIONE	IMPORTO
25,00	ESENTE	25,00

PAGAMENTO EFFETTUATO E. 25,00

UTENZA :

VI SUBISSIAMO DI AUGURI

La clonazione… come agiscono i malviventi?

7 Sniffing

Sul fronte delle transazioni in rete, accade che esperti di pirateria informatica intercettano le coordinate di pagamenti fatti con le carte di credito utilizzando poi le stesse tracce per fare ulteriori acquisti all'insaputa del vero proprietario.

La clonazione… come agiscono i malviventi?

8 Boxing

I malviventi arrivano a frugare nella cassetta della posta per sottrarre le carte di credito inviate dalle Banche/Circuiti carte di credito ai loro clienti.

La clonazione… come agiscono i malviventi?

9 Phishing

Al vostro indirizzo di posta elettronica potrebbe arrivare una email che, attraverso qualche stratagemma (ad esempio, simulando una email ufficiale della vostra banca), vi porti ad inserire i vostri dati personali e quelli relativi alla vostra carta di credito.

… per chi possiede ed utilizza una carta bancomat e/o di credito

- **Firmate** la carta sul retro appena la ricevete;
- **Custodite la carta** con la massima cura;
- Quando la carta di credito o il bancomat e il successivo codice P.I.N. vengono **recapitati a casa per posta**, controllate che le buste siano integre e che siano della vostra banca (o di chi emette la carta di credito);
- Verificate che non vi siano alterazioni o rotture del cartoncino che contiene la carta. In ogni caso, diffidate di buste bianche inviate con posta prioritaria o con francobolli (di solito sono buste con la tassa già pagata).

… per chi possiede ed utilizza una carta bancomat e/o di credito

- **Memorizzate il codice PIN senza trascriverlo:** il PIN non dovrà mai essere conservato insieme alla carta;
- Portate sempre con voi il **numero telefonico fornito dall'Emittente della carta (Banca/circuito carta di credito carta di credito) per bloccarla** in caso di furto o smarrimento.

… per chi possiede ed utilizza una carta bancomat e/o di credito

- Tenetevi sempre aggiornati sui limiti di prelevamento e pagamento della carta;
- Quando utilizzate la carta in un esercizio commerciale, è consigliabile consegnarla direttamente alla cassa e averla sempre sott'occhio.

Consigli generali…

… per chi possiede ed utilizza una carta bancomat e/o di credito

- Se ricevete una **email simile ad una comunicazione ufficiale della vostra banca** che vi suggerisce di inserire i vostri dati personali e quelli relativi alla vostra carta di credito, non rispondete mai!

Avvertite subito la Banca o le forze dell'ordine (**113** o **112**) avendo l'accortezza di non cancellare l'e-mail.

Estratto conto

- controllate che arrivi a casa tutti i mesi;
- verificate regolarmente la lista dei movimenti. In caso di operazioni “sospette”, è opportuno contattare la propria banca con la massima tempestività;
- conservare le ricevute di pagamento per poter rilevare eventuali spese non autorizzate;
- fate uso, per quanto vi è possibile, delle soluzioni di **home banking** che le Banche offrono ai Clienti per verificare i movimenti in tempo reale, via internet.

DATA 02/04/08 ORA 12:50
NUMERO SPORTELLO 3088
NUMERO OPERAZIONE 00191

DATA VALUTA IMPORTO

RICARICA CARTA PREPAGATA
21/11/07 21/11/07 EURO 406,50+

PAGAMENTO ON LINE
23/11/07 21/11/07 EURO 48.54-

PAGAMENTO DA POS UFFICIO POSTALE
10/12/07 10/12/07 EURO 9,00-

PRELIEVO SU ATM POSTE
29/12/07 28/12/07 EURO 50,00-

COMMISSIONI
29/12/07 28/12/07 EURO 1,00-

RICARICA CARTA PREPAGATA
21/03/08 21/03/08 EURO 50,00+

RICARICA CARTA PREPAGATA
31/03/08 31/03/08 EURO 20,00+

SALDO CONTABILE
02/04/08 02/04/08 EURO 367,96+

SALDO DISPONIBILE
02/04/08 02/04/08 EURO 367,96+

MUTUO BANCOPOSTA
SPECIALE SPREAD 0,85%
FINO AL 30 GIUGNO 2008

- iscrivetevi al servizio fornito da quasi tutte le Banche/Circuiti carte di credito, spesso a titolo gratuito, che trasmette un SMS in tempo reale al numero di cellulare comunicato dal Cliente in seguito a qualsiasi transazione avvenuta sulla vostra carta bancomat e di credito. Il servizio consente di bloccare in tempi rapidi l’eventuale ripetersi di transazioni non consentite.

Alcuni consigli per i commercianti…

- **Controllare frequentemente il macchinario P.O.S**. per impedirne la manomissione e la modifica da parte di qualcuno che ha possibilità di accesso all'apparecchio. Con i P.O.S. di nuova generazione la manomissione è pressoché impossibile!

- Se **sospettate che un cliente ha utilizzato una carta clonata**, confrontare il numero della carta di credito che compare sul supporto plastico con quello (15 o 16 cifre) stampato dal P.O.S. sullo scontrino subito sotto la data e l'ora della transazione. A volte è preceduto dalla lettera "C", ma se il dato è difforme significa che la carta è clonata.

N.B. Attualmente, per legge, sullo scontrino del POS il numero di carta di credito appare solo per le ultime 4 cifre, al posto delle altre appaiono 12 asterischi

Come accorgersi che lo sportello automatico è stato manomesso?

- Verificare che sulla fessura dove viene inserita la carta bancomat non vi siano resti di silicone o profili aggiuntivi posticci (ovvero non perfettamente aderenti alla struttura dello sportello);

- Verificare che nell'apposita fessura per l'introduzione di auricolare per non vedenti e, comunque, in altre parti dell'ATM non siano inseriti dispositivi ottici quali telecamere.

Come accorgersi che lo sportello automatico è stato manomesso?

- Prestare attenzione ad inusuali fogli, pezzi in plastica aggiuntivi, porta-depliant, residui di colla o mastice;

- Verificare che non ci siano graffi o ammaccature sul perimetro della tastiera, che potrebbero essere state inavvertitamente procurate dai malviventi al momento dell'inserimento della falsa tastiera.

Quando effettuate una qualunque operazione presso lo sportello, quali precauzioni adottare?

- Diffidate di sconosciuti disposti ad aiutarvi ad eseguire le operazioni;
- Quando inserite il codice PIN, è consigliabile celare il codice che si sta per digitare(ad esempio utilizzando la mano libera o un foglio di carta o il portafoglio o altro);
- Se sbagliate per 3 volte consecutive la digitazione del PIN la carta verrà trattenuta all'interno dello sportello. In questo caso avvisate la banca che provvederà a ridarvi una nuova carta.

Quando effettuate una qualunque operazione presso lo sportello, quali precauzioni adottare?

- Se la carta si inceppa nell'apparecchio di prelievo, non abbandonate per nessun motivo lo sportello. Avvisate le forze dell'ordine (113 o 112) e comunicate alla banca/circuito carta di credito il blocco della vostra carta perché molto probabilmente l'inceppamento è di origine dolosa!
- Se vi accorgete che il trascinamento della carta nell'apposita fessura avviene con un movimento discontinuo, detto "a tremarella", sia in entrata che in uscita, non preoccupatevi! Si tratta di un ulteriore sistema di protezione della carta;
- Non gettate la ricevuta alla fine della transazione.

Quando effettuate un pagamento in un esercizio commerciale…

- non perdete mai di vista la carta;
- non cedete mai la vostra carta e il vostro PIN ad altre persone, neanche al commerciante che afferma di non avere l'apparecchio P.O.S. con sé, semmai offritevi di accompagnarlo;

- diffidate di chi non ha il P.O.S. a vista o fa più strisciate;
- prima di firmare una ricevuta d'acquisto, controllate che l'importo indicato sia quello giusto;
- non gettate le ricevute degli acquisti.

Acquisti su Internet: come evitare le frodi

- controllate se sul sito web è indicato un indirizzo fisico e telefonico dove contattare l'azienda;
- assicuratevi che i siti utilizzino protocolli di sicurezza che permettano di identificare l'utente. Il più diffuso è il Secure Socket Layer (SSL): generalmente durante la transazione compare un'icona con un **lucchetto** che sta a significare che in quel momento la connessione è sicura;

- assicuratevi che il sito su cui si digitano i dati sia **criptato**: il sito che usa dati criptati si riconosce perché nell'indirizzo compare "**https**" al posto di "**http";**
- utilizzate siti conosciuti o che abbiano un minimo di credibilità sia per quanto riguarda il prodotto venduto, che la solidità del marchio;
- se avete dubbi, utilizzate un metodo di pagamento alternativo oppure utilizzate una carta prepagata;
- stampate e conservate sempre le ricevute dei pagamenti e le clausole dei contratti: potrebbero risultare utili in caso si voglia contestare l'acquisto.

… cosa fare?

Bloccate immediatamente la carta telefonando al numero che vi è stato fornito dalla vostra banca/ circuito carta di credito.

Di seguito trovate i numeri telefonici verdi (gratuiti) delle società emittenti più diffuse a cui telefonare per segnalare eventuali dubbi o bloccare la carta in caso di furto o smarrimento.

Servizi Interbancari (Carta SI): 800 151616	**Setefi: 800 825099**
American Express: 800 864046	**Banca Fineco: 800 525252**
Top Card: 800 900910	**Banca Sella: 800 822056**
Diner's: 800 864064	**Findomestic: 800 866116**
Agos Itafinco: 800 822056	**Citibank: 800 407704**
Deutschebank: 800 207167	

Se avete il sospetto di essere stati vittima di una frode

- Tenete con voi la carta per attestare che non l'avete smarrita e non vi è stata sottratta;
- Procedete con una denuncia alle forze dell'ordine, allegando una copia dell'estratto conto in cui avete evidenziato le operazioni fraudolente eventualmente effettuate sul vostro conto;
- Inviate una copia della denuncia e dell'estratto conto evidenziato alla banca/società emittente, sia via fax sia per posta raccomandata.

Per concludere…

I mezzi di pagamento elettronici sono strumenti di grande utilità, il cui uso è ormai divenuto pratica comune in moltissime delle nostre attività quotidiane.

Utilizzarli in maniera corretta ed intelligente, anche seguendo questi semplici consigli, vi consentirà di ridurre al minimo i rischi di truffe o raggiri.

Grazie…

al contributo
del Gruppo di Lavoro
composto dai rappresentanti di:

Questura di Firenze e Bassilichi