Questura di Firenze

TIPOLOGIE DI FRODI

Bancomat e carte di credito offrono,un sistema di **pagamento comodo e relativamente sicuro**, anche su Internet, ma è opportuno adottare alcune cautele per evitare di essere vittime di frodi.
La diffusione dei sistemi di pagamento elettronici ha infatti ampliato la casistica criminale connessa alla contraffazione dei supporti utilizzati per effettuare pagamenti ed acquisti mediante carte di credito e debito.

Lebanese Loop

- **sullo sportello di prelievo automatico viene applicato un dispositivo che, una volta inserita la carta la trattiene** in modo che il distributore non riesca più a restituirla
- **il cliente non può completare la transazione** né riavere la carta.
- 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 cosi di memorizzarlo
- **dopo l'allontanamento della vittima il criminale può recuperare la carta** e utilizzarla con il pin appena memorizzato

Lo **skimmer**

- **E' un sistema molto più diffuso e soprattutto molto più efficace del "Lebanese Loop",** poiché il cliente utilizza normalmente lo sportello automatico senza rendersi conto che i dati della nuova carta vengono copiati.
- **Per carpire la banda magnetica viene utilizzato lo skimmer,** uno degli apparecchi più utilizzati per duplicare le carte: un lettore che cattura i dati della banda magnetica con la semplice "strisciata" della carta di credito su di esso.
  - ✓ 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 carte di creditoI
  - ✓ 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.
  - ✓ viene montato nella fessura di inserimento della carta
- **Per appropriarsi invece del codice PIN**, che non è in alcun modo ricavabile dalla banda magnetica, viene utilizzata generalmente
  - ✓ una microtelecamera nascosta, montata sul pannello di controllo (ad es. in un porta brochure), che filma la digitazione del codice PIN da parte del proprietario della carta.
  - ✓ una finta tastiera applicata su quella reale

Frodi tramite lettore (P.O.S.) fornito dalle società

- è necessario che il truffatore entri in possesso, anche solo per alcuni istanti, della carta di credito del cliente, possibilmente lontano dalla sua vista.
- **l**a carta viene passata prima nel terminale POS e successivamente nello **skimmer** per "catturare" i dati presenti sulla banda magnetica.

Trashing

- i truffatori utilizzano gli scontrini delle carte di credito che talvolta i possessori gettano via dopo un acquisto
- è opportuno tenere la matrice per controllare la regolarità dell'estratto conto e, soprattutto, per non dar modo ad altri di impossessarsi dei dati di identificazione della carta.

Sniffing:
Riguarda le transazioni fatte in rete: esperti di pirateria informatica intercettano le coordinate di pagamento fatte con le carte di credito, utilizzando poi le stesse tracce per fare ulteriori acquisti all'insaputa del vero proprietario.

Boxing.
Consiste nella sottrazione delle carte di credito inviate dalle banche ai loro clienti.

Alterazione del POS
Viene aperto il dispositivo del POS al cui interno viene istallato un microprocessore che registra i codici della carta di credito o il pin della carta. Il microprocessore viene poi prelevato dal pos ed utilizzato dal criminale per ricreare nuove carte di credito.

Carte smarrite o rubate
Il truffatore utilizza una carta di credito rubata o smarrita prima che il titolare se ne accorga e la blocchi.

I dati acquisiti con la frode possono essere copiati direttamente sulla banda magnetica della carta falsificata oppure possono essere rivenduti a criminali che si occupano della successiva codifica.
Le carte a questo punto vengono stampate in modo tale che i dati sulla banda magnetica coincidano con quelli sul fronte della carta.
Una carta falsificata può essere venduta dalle organizzazioni criminali per una cifra intorno ai 500 euro, in seguito verrà utilizzata negli esercizi commerciali.

CONSIGLI PER I CITTADINI

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 all'interno non vi siano alterazioni o rotture del cartoncino** che contiene la carta
- **diffidate di buste bianche inviate con posta prioritaria o con francobolli** (di solito sono buste con la tassa già pagata).

ALLO SPORTELLO

- **Osservate l'apparecchiatura alla ricerca di anomalie e modifiche**.
  - **Controllate la fessura d'ingresso della carta bancomat**:se sporge, se si muove o si stacca, se è di colore differente a quelli della banca, se ci sono resti di silicone potrebbe significare che è stata coperta con uno "skimmer"
  - **Controllate la tastiera:**
    - ✓ sulla verticale o diagonale della tastiera può esserci una microtelecamera nascosta in un foro o in un contenitore
    - ✓ verificare se anche la tastiera è ben fissa: spesso i truffatori sovrappongono una loro tastiera per catturare il codice Pin; in questo caso c'è un gradino di un paio di millimetri
  - **Prestate attenzione ad inusuali dispositivi, fogli, pezzi in plastica aggiuntivi di colore diverso, porta-depliant, residui di colla o mastice** sugli sportelli bancomat.);
- **Nel caso del dubbi:** non introdurre la tessera e non inserire il Pin. Allontanarsi e chiamare le forze dell'ordine.
- **Digitazione del Pin:** digitate il codice nascondendo con il palmo dell'altra mano l'operazione e accertatevi che nessuno vi stia osservando
- **Non accettare aiuto da estranei**, anche se si identificano come personale della banca, piuttosto, se possibile, entrate nella banca e fate presente il problema.
- **Se il distributore non restituisce la carta** non vi allontanate dallo sportello, avvisate le forze dell'ordine (113) e il numero verde apposito
- **Non gettate la ricevuta alla fine della transazione.**

In maniera analoga si cerca di accedere ai dati dei PIN mediante l'accesso alle porte di sportelli bancomat: **per accedere ai locali solitamente basta infatti l'inserimento della carta per fare aprire la porta di uno sportello bancomat, non serve digitare il PIN.**

CON LE CARTE DI CREDITO

- **non perdete mai di vista la carta di credito**, soprattutto durante i pagamenti
- **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
- **non custodite il PIN insieme alla carta** (ad esempio nel portafoglio o nella borsa); meglio memorizzare il codice
- **firmate la carta sul retro appena la ricevete.**
- **estratto conto:**
  - **controllatelo ogni mese** poiché è l'unico modo per accorgervi di eventuali spese mai effettuate
  - **controllate che arrivi regolarmente tutti i mesi**: il truffatore potrebbe rubarlo dalla cassetta della posta per utilizzare poi i dati contenuti in esso.
  - **fate uso, per quanto possibile, delle soluzioni di home banking,** che le banche mettono a disposizione per controllare - quasi in tempo reale - il proprio estratto conto, in modo da bloccare, tempestivamente, la carta qualora si disconoscessero delle spese addebitate;
- **addebiti impropri:** se vi arriva un estratto conto con addebiti impropri è bene denunciare alle forze dell'ordine la clonazione della carta, disconoscendo le spese addebitate
- **e-mail:** al vostro indirizzo di posta elettronica potrebbe arrivare un'email che, attraverso qualche stratagemma (ad esempio simulando un'email ufficiale della vostra banca), vi porti ad inserire i vostri dati personali e quelli relativi alla vostra carta di credito:
  - non rispondete mai a questo tipo di email e non inserite i vostri dati personali.
  - avvertite la banca o le forze dell'ordine avendo l'accortezza di non cancellare l'e-mail
- **acquisti**
  - diffidate di chi non ha il POS a vista o fa più strisciate
  - prima di firmare una ricevuta d'acquisto presso un negozio controllate che l'importo indicato sia quello giusto.
  - non gettate e non lasciate incustodite le ricevute degli acquisti: ricordate che sulla ricevuta è stampato sia il numero di carta che la data di scadenza
  - sarebbe utile abilitare il servizio di avviso sul cellulare che informa immediatamente di qualsiasi utilizzo della carta o bancomat; in questo modo l'utente può verificare in tempo reale se la spesa è stata sua e bloccare immediatamente la carta.
- **bloccate immediatamente la carta** quando vi accorgete di non esserne più in possesso
- **tenetevi sempre aggiornati** sui **limiti di prelevamento e pagamento** della propria carta

UTILIZZO DELLA CARTA DI CREDITO SU INTERNET

Per fare acquisti o operazioni attraverso la rete Internet di solito viene richiesto dal sito interessato:

- **nome e cognome del titolare della carta di credito**
- **scadenza della carta**
- **Cin o numero di sicurezza** che, di solito, si trova dietro la carta di credito.

Per evitare frodi nel caso di acquisti sul web

controllate se sul sito web è indicato un indirizzo fisico e telefonico dove contattare l'azienda. Procedete con estrema cautela qualora sia indicato solo un numero di cellulare o un indirizzo email

- assicuratevi che i siti in questione utilizzino **protocolli di sicurezza** che permettano di identificare l'utente. Il più diffuso è il *Secure Socket Layer* (SSL): generalmente durante la transazione, in basso a destra della finestra, 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"** anzichè **http://,** evitando così a pirati informatici di carpire i dati personali mediante intrusione telematica
- **utilizzate siti conosciuti** o che abbiano un minimo di credibilità sia per quanto riguarda il prodotto venduto, che la solidità del marchio
- **utilizzate i motori di ricerca:** spesso è possibile trovare indicazioni sull'affidabilità di un negozio *online* tra commenti e messaggi di utenti che hanno già acquistato in passato
- **se avete dubbi** circa l'affidabilità di un negozio 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 utilili in caso si voglia contestare l'acquisto.

Cosa fare se sospettate di essere stati vittima di una frode

- **Bloccate immediatamente la carta** telefonando al numero blocchi
- **Informate la banca**
- **Chiedete e controllate l'estratto conto** e se vi sono spese che non riconoscete , evidenziatele.
- **Tenete con voi la carta** (salvo il caso di Lebanese Loop**)** 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 con le voci precedentemente evidenziate, facendo presente di aver sempre custodito carta e pin con la massima cura e disconoscendo le operazioni fraudolente eventualmente effettuate sul vostro conto.
- **Inviate una copia della denuncia e dell'estratto conto evidenziato alla società emittente** sia via fax che per posta raccomandata (non inviare mai gli originali, sempre le copie)

Come bloccare la propria carta di credito

Questi sono i numeri telefonici verdi (gratuiti) delle società della carte di credito più diffuse a cui telefonare per segnalare eventuali dubbi o bloccare immediatamente la carta in caso di furto o smarrimento.

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

CONSIGLI PER I COMMERCIANTI

E' sempre opportuno :

- **in caso di sospetto di utilizzo di carta di credito 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 èclonata;
- **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.