

INTERNET E PAGAMENTI ELETTRONICI: COME DIFENDERSI DALLE FRODI

Ecco alcuni consigli del Movimento Difesa del Cittadino



Oggi giorno, noi consumatori siamo bombardati da nuovi mezzi di pagamento: carte di credito, trasferimenti, e-banking, pagamenti via cellulare, denaro elettronico.

Ma riceviamo spiegazioni appropriate su come utilizzarli? Conosciamo tutti i rischi quando firmiamo un contratto utilizzando questi mezzi di pagamento? Sappiamo se, nel caso subiamo una frode, la banca che ci sta offrendo questi mezzi di pagamento si solleva da qualsiasi responsabilità?

CARTE DI CREDITO E BANCOMAT

Le carte di pagamento sono strumenti che consentono di acquistare beni e servizi senza utilizzo del contante: tramite addebito immediato sul proprio conto corrente (Bancomat) o differito (carta di credito). Consentono anche di prelevare contanti dagli sportelli attraverso un codice identificativo (PIN).

PRO – possibilità di prelevare contante presso qualsiasi sportello bancario e di acquistare nei negozi con dispositivo POS; per le carte di credito anche: utilizzo all'estero, pagamenti a distanza (es. per acquisti tramite Internet).

CONTRO - rischio clonazione, che avviene attraverso la duplicazione della carta di pagamento ad opera di chi intende farne un uso illecito, dopo averne letto i dati.

COME DIFENDERSI DALLE FRODI



Allo sportello Bancomat

- 1) Coprire sempre la mano quando si digita il codice.
- 2) Fare attenzione a non essere visti quando si digita il codice.
- 3) Attenzione a qualsiasi anomalia riscontrata allo sportello e nei sistemi elettronici utilizzati (es. tastiera, spazio in cui si infila la tessera magnetica).
- 4) Meglio recarsi agli sportelli Bancomat nelle ore di apertura della banca: in caso di malfunzionamento o dubbi potete chiedere al personale della banca.
- 5) Controllare estratto conto e movimenti della carta ogni settimana.

Al pagamento Pos

- 1) È consigliabile fissare il plafond di spesa mensile della carta al minimo per limitare i danni in caso di clonazione.

- 2) Controllare l'estratto conto della carta ogni settimana.
- 3) Chiedere eventualmente alla propria banca il servizio SMS di avviso su ogni movimento della carta.
- 4) Utilizzare eventualmente carte di credito ricaricabili.

In caso di clonazione

Provvedere immediatamente al blocco della carta e alla relativa denuncia!

E-BANKING

Il mercato dell'home banking è in continua crescita: in Italia sono circa 12 milioni i conti abilitati a operare via Internet e che danno la possibilità al cittadino di controllare il saldo e i movimenti del proprio c/c, effettuare bonifici e pagamenti delle utenze.

PRO - costi ridotti e facilità/libertà nella consultazione del proprio conto.

CONTRO - crescente aumento delle truffe telematiche, con furti di password e codici segreti (il famigerato "phishing").

COME DIFENDERSI DALLE FRODI

- 1) Installa e mantieni aggiornati sistema operativo e software di protezione (antivirus e antispyware), effettuando le scansioni periodiche e proteggendo il traffico in entrata e in uscita dal computer con programmi di filtraggio del flusso di dati (firewall).
- 2) Durante la navigazione in Internet, installa solo programmi di cui puoi verificare la provenienza.
- 3) Verifica l'autenticità della connessione con la tua banca, controllando il nome del sito nella barra di navigazione. Se è presente, clicca due volte sull'icona del lucchetto (o della chiave) in basso a destra nella finestra di navigazione e verifica la correttezza dei dati visualizzati.
- 4) Controlla regolarmente le movimentazioni del tuo conto corrente per assicurarti che le transazioni riportate siano quelle realmente effettuate.
- 5) Fai attenzione a eventuali anomalie rispetto alle abituali modalità con cui ti viene richiesto l'inserimento dei dati personali sul tuo sito di home banking.
- 6) Privilegiare conti on line con la One Time Password (OTP), uno strumento delle dimensioni di un portachiavi, che alla pressione di un pulsante visualizza un codice ogni volta nuovo e diverso da utilizzare come password di conferma delle disposizioni.

PHISHING

Il phishing è una frode informatica realizzata con l'invio di e-mail contraffatte, con mittenti autorevoli e reali, che linkano falsi siti clonati (es. Poste, Banca Intesa, Paypal o Ebay). È finalizzata all'acquisizione per scopi illegali di dati riservati come dati di accesso a sistemi bancari e interbancari.

COME DIFENDERSI DALLE FRODI

- 1) Non cliccare su link presenti in e-mail sospette che potrebbero condurre a siti contraffatti, molto simili all'originale.
- 2) Diffidare di qualunque richiesta di dati relativi a carte di pagamento, chiavi di accesso all'home banking o altre informazioni personali: la banca non chiederà mai queste informazioni via e-mail!
- 3) Diffidare di qualsiasi messaggio (di posta elettronica, siti web, contatti di instant messaging, chat o peer-to-peer) inviti a scaricare programmi o documenti dei quali si ignora la provenienza.
- 4) Nel dubbio che una e-mail possa essere di Phishing, quindi non originale, cancellarla e comunque non cliccare assolutamente i link!

MDC sta sviluppando un **progetto sulle frodi nei mezzi di pagamento** con il sostegno della Commissione Europea in collaborazione con ADICAE e altre associazioni europee di consumatori.