



Se sei titolare di una carta di pagamento oppure un esercente di un'attività commerciale, in questo pieghevole troverai tanti utili consigli pratici e accorgimenti che potrebbero risultare preziosi per prevenire le frodi con carte di credito o di pagamento.

Consigli di sicurezza per l'uso della carta di credito su internet.

Verifica che l'URL presente sulla barra degli indirizzi del browser inizi con **https://** nella pagina in cui vengono inseriti i dati della carta di pagamento. Se hai dubbi circa l'affidabilità di un negozio, utilizza un metodo di pagamento alternativo oppure una carta prepagata.



Non inserire mai il tuo numero di carta su siti o pagine non protette da sistemi di sicurezza, riconoscibili dalla certificazione e dal lucchetto (o chiave) che appaiono sempre nella banda superiore del browser.

Effettuato l'ordine, verifica di averne ricevuto una copia e di aver ricevuto l'email con il numero di transazione effettuato mediante carta di pagamento.

Non fornire a nessuno, telefonicamente o via e-mail, il numero di carta di credito oppure il codice PIN della carta di pagamento.

Stampa e conserva sempre le ricevute dei pagamenti perché sono indispensabili per contestare l'acquisto.

Consigli per l'esercente dotato di POS.

l'aspetto estetico è il primo elemento da valutare: una carta clonata in alcuni casi è fatta in maniera grossolana e quindi facilmente riconoscibile. Ad esempio:



verifica che le cifre poste in rilievo riferite al nome del titolare, data di emissione e di scadenza, siano chiare ed in linea;

controlla se sulla carta è posta la firma del titolare: se manca, potrebbe essere falsa;

confronta sempre il numero della carta di credito con quello dello scontrino del Pos; se il dato è difforme significa che la carta è stata clonata.

richiedi un documento d'identità all'acquirente, soprattutto se questo manifesta atteggiamenti sospetti;

controlla la presenza del sigillo di sicurezza posto sull'apparecchiatura POS, se manca è necessario contattare l'acquirer perché vi è un'alta probabilità che il dispositivo sia stato manomesso.

Alcuni consigli per non rimanere vittima di azioni fraudolente

le carte ed i loro codici segreti non devono mai essere conservati insieme. Se possibile memorizza i codici e, in ogni caso, non riscriverli mai su bigliettini o foglietti di carta;

non rivelare a nessuno i codici associati alle tue carte di pagamento;

scegli una carta che offra il **servizio gratuito di invio notificazione delle operazioni tramite sms;**

presta attenzione a **non essere osservato** durante la digitazione del codice "PIN";

firma la carta sul retro appena la ricevi;

controlla la regolarità degli invii degli estratti conti della carta: in caso di anomalie non esitare a contattare l'emittente, perché potresti essere vittima di trashing.



Consigli di sicurezza per l'uso delle carte presso i distributori automatici di contante.

Fai attenzione alle persone in prossimità del distributore. Se hai sospetti non usarlo.



Se noti pannelli inusuali o microtelecamere fallo immediatamente presente alla

banca o chiama subito il 112.

Non accettare aiuto da estranei, anche se si identificano come personale della banca, piuttosto entra nell'istituto per far presente il malfunzionamento.

Se il distributore non restituisce la carta contatta in ogni caso il numero verde apposito.

Non disperdere la ricevuta alla fine della transazione.



Non perdere mai di vista la tua carta di credito durante i pagamenti. Diffida da chi non ha il POS a vista o fa più strisciare. Questo accorgimento è fondamentale per evitare lo skimming.

Conserva gli scontrini dei prelievi e dei pagamenti effettuati con carta di credito, in modo da poter verificare dall'estratto conto le somme addebitate e quelle effettivamente spese.

Non gettare o lasciare incustodite le ricevute degli acquisti: ricorda che su di esse è indicato il numero e la data di scadenza della carta!

Prima di firmare una ricevuta d'acquisto presso un negozio controlla che l'importo indicato sia corretto.

...ricordati ancora.

In caso di smarrimento o furto di una carta di pagamento telefona il numero verde di assistenza clienti per bloccare la carta. **non conservare il pin all'interno del portafoglio.**



Cambia spesso le tue password utilizzate per accedere ai servizi on-line;

non cedere mai la carta di credito e il pin ad altre persone.

Utilizza, se possibile, **carte prepagate** non direttamente collegabili al conto corrente per gli acquisti on-line.

Durante la digitazione del pin, sposta l'apparecchio rispetto alla posizione proposta.

Se di notte noti più persone nei pressi di uno sportello bancomat, non esitare a chiamare il 112, potrebbero essere intenti a perpetrare un reato.



Il Comando Carabinieri più vicino è la Stazione di Fontanelle (TV)

Via Vallonto nr.13

Telefono 0422/749306

Vediamo da vicino alcuni metodi utilizzati per compiere le truffe

Telecamere su sportello automatico. Per entrare in possesso del PIN della carta in alcuni casi i malviventi installano una microcamera sopra lo sportello, che legge il codice digitato dal malcapitato.

Skimming. Lo skimmer è un dispositivo che viene montato nella fessura di inserimento della carta nello sportello bancomat: serve a leggere ed immagazzinare le bande magnetiche delle carte che passano.

Trashing. Non buttare le ricevute o gli scontrini di acquisti con carte di credito: possono essere utilizzate da malviventi in combinazione con sistemi di telecamere.

Manomissione del POS. Può avvenire all'interno di un esercizio commerciale, dove nel POS viene installato (ovviamente a insaputa del commerciante) un microprocessore che registra i codici delle carte di credito.

Sniffing. Uno dei metodi più utilizzati, soprattutto su carte prepagate, è l'intercettazione delle coordinate bancarie dei pagamenti on-line. Questi dati, presi su siti che agli utenti sembrano sicuri, vengono riutilizzati per fare acquisti all'insaputa del vero proprietario.

Phishing. Si tratta di e-mail che simula una comunicazione ufficiale di Poste o banche, e invitano i clienti ad inserire i dati della propria carta. non aprire mai mail di questo genere.



Boxing. Non sono rari i casi in cui vengono frugate cassette della posta per prendere le carte di credito che le banche inviano ai clienti.

www.carabinieri.it/cittadino

AIUTATECI AD AIUTARVI



Nel dubbio, chiamate sempre il



vi consiglieremo
cosa fare!



www.carabinieri.it/social/



CARTE DI CREDITO E FRODI VIA WEB ECCO COME SALVARSI!

#POSSIAMOAIUTARVI

Suggerimenti e consigli per mettere la sicurezza al primo posto

NUMERI VERDI PER IL BLOCCO DELLE CARTE PIÙ DIFFUSE

CARTA BANCOMAT :

800-822056 (per tutte le Carte BANCOMAT);

CARTASI' :

800-151616 (dall'Italia);

+390234980020 (dall'estero);

1-800-4736896 (dagli USA)

CARTAPOSTAMAT/MAESTRO

800 - 652653; dall'estero +39 - 0492100148

CARTA POSTEPAY

800 - 902122; dall'estero +39 - 0492100149

CARTA VISA

800 - 819014 (dall'Italia)

VIACARD

840/043043 (numero valido anche per furto/smarrimento dell'apparato Telepass).



LE FRODI CON CARTA DI CREDITO

I pagamenti online sono utilizzati da molte persone che per comodità, per risparmiare o per sbrigare più velocemente le proprie pratiche, scelgono di fare transazioni su Internet con la propria carta di credito. Oggi queste operazioni risultano essere molto sicure nonostante ciò per diminuire il rischio di rimanere vittima di truffe è importante prestare attenzione. Talvolta, ricorrere a siti di pagamento sicuri potrebbe non bastare per proteggersi dalle frodi, in quanto i metodi delle truffe online

sono sempre più ingegnosi e non riguardano soltanto le operazioni su Internet.

Cosa fare se sospetti di essere stato vittima di una frode?

Blocca immediatamente la carta telefonando al numero verde per i blocchi.

Controlla l'estratto conto e contatta l'emittente in caso di spese sospette.

Hai a disposizione 90 giorni per recarti presso il Comando Carabinieri più vicino per sporgere una denuncia-querela allegando una copia dell'estratto conto con le voci precedentemente evidenziate, facendo presente di aver sempre custodito carta e pin con la massima cura.

Invia una copia della denuncia e dell'estratto conto alla società emittente sia via fax che per posta raccomandata (non inviare mai gli originali, sempre le copie).

L'istituto emittente richiede copia della denuncia entro pochi giorni dal blocco della carta; in questo modo potrà verificare e riconoscere l'assenza totale di responsabilità del titolare per le spese effettuate con la tua carta dopo il blocco.



Il Comando Carabinieri più vicino è la Stazione di Fontanelle (TV)

Via Vallonto nr.13

Telefono 0422/749306