

# Guida alla sicurezza, in banca

PER GESTIRE  
AL MEGLIO  
I PAGAMENTI  
ELETTRONICI





Caro Lettore,

PattiChiari è il Consorzio attraverso il quale l'industria bancaria italiana lavora per **semplificare l'uso dei prodotti bancari e per migliorare la cultura finanziaria dei propri clienti** affinché ciascuno possa compiere scelte consapevoli, informate e adatte alle proprie esigenze.

Con questo obiettivo abbiamo definito un insieme di strumenti e di regole che abbiamo chiamato **“Impegni per la Qualità”**, alcuni dei quali sono dedicati al tema della sicurezza.

Questa **Guida** in particolare vuole informarti sugli strumenti che le banche aderenti a PattiChiari ti mettono a disposizione per gestire con ancor più sicurezza le operazioni on-line, indicandoti cosa fare per proteggerti contro le frodi informatiche e quelle effettuate con le carte di pagamento.

**Buona Lettura!**

## La sicurezza è semplice

Le **carte di debito** (ad esempio le carte Bancomat), le carte di credito e quelle prepagate ti consentono di effettuare i tuoi acquisti e prelievi di denaro, in Italia come in tutto il mondo a seconda del circuito di pagamento collegato alla carta, liberandoti dalla necessità - e dai rischi - di portare con te troppi contanti.

Con i servizi di **internet** e **phone banking** puoi informarti e operare con la tua banca (ad esempio chiedendo il saldo e i movimenti del conto, oppure facendo bonifici, ricariche telefoniche e operazioni di borsa), dovunque tu sia e in qualsiasi momento.

Si tratta di strumenti divenuti ormai di uso quotidiano, molto utili e sempre più semplici da usare, ma che richiedono notevoli investimenti alle banche per la continua evoluzione delle complesse tecnologie informatiche che sono alla base del loro buon funzionamento, e soprattutto della loro sicurezza.

Un argomento, quest'ultimo, su cui **ciascuno deve fare la sua parte**:

- **la tua banca**, offrendoti gli strumenti per gestire senza problemi i pagamenti e i prelievi tramite le carte e le operazioni eseguite con i canali remoti di internet banking o di phone banking;
- **tu stesso**, adottando i semplici accorgimenti suggeriti in questa Guida.

Anche tu, infatti, puoi avere un ruolo importante per evitare che dei truffatori approfittino in modo illegale delle tue informazioni riservate utilizzandole a tuo discapito. Vediamo come.

Iniziamo con qualche raccomandazione generale, **3 semplici accorgimenti per la tua sicurezza.**



**Le informazioni e gli strumenti con cui accedi ai servizi della tua banca (password, PIN, codici, carte, ecc.) sono strettamente personali. Custodiscili sempre con la massima attenzione e ricorda che ne sei responsabile!**

Ricorda che la banca può contattarti telefonicamente, via e-mail o sms per darti informazioni, ma non ti chiederà mai di fornirle direttamente i tuoi codici di accesso ai servizi.



**Controlla regolarmente i tuoi estratti conto.**

In questo modo puoi assicurarti che le operazioni riportate siano quelle realmente effettuate. In caso contrario contatta subito il call center della tua banca o rivolgiti alla tua filiale.



**Nei casi in cui riscontri anomalie nei servizi o ritieni di essere stato vittima di una frode rivolgiti immediatamente alla banca, attraverso i contatti che ti ha fornito.**

A tale scopo, segnati e tieni sempre a portata di mano i numeri di riferimento della tua banca, come ad esempio il numero verde del call center.

Per qualsiasi evenienza ricorda che il call center della tua banca ti fornisce supporto nell'utilizzo in sicurezza dei servizi della banca ed è accessibile in modo semplice e immediato sia da casa che dal tuo cellulare.

## L'internet banking

L'internet banking è molto comodo perché ti dà la possibilità di entrare nella tua banca direttamente da un computer, per avere le informazioni che ti servono o effettuare operazioni dispositive on-line, ma occorre utilizzarlo seguendo alcune semplici accortezze che ti presentiamo in questa Guida.

Le banche da sempre mantengono una forte attenzione per poterti garantire i migliori sistemi di protezione contro le frodi in Internet.

**Con l'obiettivo di potenziare ulteriormente il livello di sicurezza dell'internet banking, le banche aderenti al Consorzio PattiChiari ti offrono un ulteriore elemento di riconoscimento (spesso collegato alla consegna di un dispositivo, di una tessera, di un software da installare sul tuo PC o sul tuo cellulare), che si aggiunge all'utilizzo del codice utente e delle credenziali di accesso al servizio.**

Ti ricordiamo, infine, che per l'utilizzo dell'internet banking dovrai stipulare uno specifico contratto con la banca.

## Qualche consiglio sull'internet banking

### *Conosci bene il servizio che offre la tua banca*

- Scrivi direttamente l'indirizzo del servizio di internet banking nella barra di navigazione e non accedere mai attraverso link presenti in e-mail (anche se apparentemente provenienti dalla banca).
- Attiva i meccanismi di sicurezza, come ad esempio le notifiche o le segnalazioni via e-mail o sms, messi a disposizione dalla tua banca per il tuo conto.
- Controlla che non ci siano anomalie nelle usuali procedure di accesso all'internet banking, ad esempio nel modo con cui ti viene richiesto di inserire i dati. Se hai qualche dubbio, avverti subito la tua banca.
- Verifica l'attendibilità del sito a cui accedi: ti basta cliccare sull'icona del lucchetto presente nel browser di navigazione (il più diffuso è Internet Explorer) e verificare che le informazioni riportate facciano riferimento a una data di scadenza ancora valida.

**In tutti questi casi, se incontri delle difficoltà o qualcosa non ti è chiaro, chiedi spiegazioni al call center o in filiale.**

### *Proteggi il tuo computer dalle insidie che circolano in rete*

- Installa adeguati software di protezione (anti-virus e anti-spyware, vedi a pag. 15) e ricordati di tenerli sempre aggiornati, così come il tuo sistema operativo e i principali programmi che utilizzi.
- Fai molta attenzione ad aprire i messaggi di posta elettronica di cui non riconosci il mittente; nel dubbio cancellali.
- Tieni sotto controllo eventuali peggioramenti delle prestazioni e della velocità del tuo computer, potrebbe essere un indice di contagio; nel caso avvia una scansione con l'anti-virus.
- Se utilizzi una postazione cui accedono anche altre persone (familiari, colleghi, amici), fai in modo che anche loro adottino queste regole di base.

**Se non sai bene come fare questi controlli, chiedi aiuto a chi è più esperto di te.**

### *Proteggi la tua identità*

- La tua identità su Internet vale tanto quanto i tuoi documenti di riconoscimento. Valuta bene le informazioni che rendi note sulla Rete, fai attenzione ad esempio ai dati personali che rendi pubblici sui siti di social networking (Facebook, Myspace, ecc.).

- Valuta con attenzione ogni richiesta di dati personali da parte di chi non conosci, soprattutto quelle connesse a offerte di lavoro, o alla proposta di “favolosi” investimenti, o alla vincita di un premio “certo”.
- Memorizza le credenziali di accesso ai servizi della tua banca e modifica frequentemente la password, se è previsto dalla procedura di autenticazione. Per una maggiore protezione, evita di attivare la funzione di salvataggio automatico.
- Tieni sempre aggiornate le informazioni personali comunicate alla banca che costituiscono gli elementi di riconoscimento per l'accesso ai servizi che hai sottoscritto.

### A CHI RIVOLGERTI IN CASO DI NECESSITÀ

Se pensi di aver subito un tentativo di frode rivolgiti subito alla tua banca, mediante i contatti che ti ha fornito. Questa ti può essere d'aiuto anche nel caso in cui hai bisogno di semplici informazioni.

Se, anche a seguito di una verifica effettuata con la banca, ritieni di aver subito una frode rivolgiti alle Autorità competenti (ad esempio Polizia o Carabinieri), che sono a tua disposizione 24 ore su 24, anche tramite un apposito sito Internet, **[www.commissariatodips.it](http://www.commissariatodips.it)**.

## Il phone banking

Il **phone banking** permette un accesso semplice e veloce a una vasta gamma di servizi che spaziano dalla semplice verifica del saldo o dei movimenti sul proprio conto, a operazioni più complesse come effettuare bonifici, ricariche telefoniche, operazioni di borsa, ecc.

Per utilizzare il servizio, dopo aver sottoscritto un apposito contratto con la banca, ti basta una semplice telefonata, che puoi fare dovunque tu sia e con “orari di apertura” molto ampi; per l’attivazione del servizio la banca ti fornirà i codici di accesso, per i quali valgono le stesse raccomandazioni che ti abbiamo presentato per l’internet banking.

Puoi operare **tramite telefono fisso o telefono cellulare**, chiamando il numero verde che ti ha dato la tua banca e seguire le istruzioni che ti vengono fornite da un risponditore automatico oppure parlare direttamente con un operatore.

## Le carte di pagamento

Le banche e i Circuiti delle carte di pagamento sono costantemente impegnati a innalzare i livelli di sicurezza degli strumenti di pagamento elettronici. Proprio con questo obiettivo, ad esempio, **è in corso la sostituzione di tutte le carte di pagamento a «banda magnetica» con quelle dotate di “microchip”**.

Per fornirti maggiore sicurezza contro le frodi o l'utilizzo indebito delle carte, le banche aderenti a PattiChiari hanno attivato appositi strumenti di controllo che potranno comportare l'invio di “avvisi”, ad esempio via sms o e-mail, sulle operazioni per le quali ritengono necessaria una tua verifica.

Infatti, **a seconda del sistema utilizzato dalla banca**, riceverai una comunicazione ogni volta che il sistema di controllo e monitoraggio della tua banca ravvisi delle operazioni “anomale” (ad esempio transazioni di importo rilevante, frequenza o dislocazione geografica delle transazioni, ecc.).

Inoltre, nel caso in cui tu chiedi il rimborso di un addebito errato o non autorizzato sulla tua carta, se la tua banca aderisce a PattiChiari potrai contare su tempi certi e veloci di risposta: è previsto infatti un termine temporale massimo di 15 giorni lavorativi per il rimborso, a partire dal momento in cui avrai presentato tutti i documenti richiesti dalla banca.

Nei casi in cui l'accertamento dell'effettivo errore o della frode - da parte della banca - comporti tempi tecnici più lunghi, l'importo ti verrà comunque accreditato entro il termine di 15 giorni, ma con la clausola "salvo buon fine".

La disponibilità delle somme non sarà pertanto definitiva fino al termine dell'istruttoria che dovrà essere conclusa dalla banca entro 120 giorni dalla data di consegna della documentazione.

Inoltre, ti ricordiamo che, per gli acquisti effettuati a distanza (ad esempio on-line), l'art. 56 del Codice del Consumo prevede che l'emittente della carta riaccrediti i pagamenti per i quali il consumatore dia prova dell'eccedenza rispetto al prezzo pattuito o dell'uso fraudolento della propria carta.

### *Qualche consiglio sulle carte di pagamento*

- Custodisci le tue carte con la massima cura e memorizza i relativi PIN senza trascriverli, in ogni caso ricorda che il PIN non deve mai essere conservato insieme alla carta.
- Quando è previsto, firma sempre le tue carte sul retro, non appena le ricevi.
- Adotta tutte le misure volte a impedire che qualcuno possa leggere e memorizzare il tuo PIN mentre lo digiti.

- Digita il tuo PIN o firma la ricevuta solo dopo aver controllato l'importo.
- Porta sempre con te, o memorizza sul cellulare, il numero telefonico che ti ha comunicato la banca per il blocco della carta.
- Non perdere mai di vista la carta al momento dei pagamenti (ad esempio al ristorante).

### *Cosa fare in caso di furto/smarrimento e clonazione della carta*

In caso di furto o smarrimento della tua carta è necessario:

- bloccare immediatamente la carta chiamando l'apposito numero telefonico (vedi box a pag. 9) che ti fornirà il codice di riferimento del blocco
- sporgere denuncia alle Forze dell'ordine. Nel caso di smarrimento la denuncia dovrà essere effettuata se vengono rilevate operazioni che non hai eseguito
- recarsi nella propria filiale per segnalare il fatto.

Nel caso in cui invece, leggendo il tuo estratto conto (oggi, nella maggior parte dei casi, puoi farlo anche con Internet) individuassi prelievi o spese che sicuramente non hai effettuato e la carta è in tuo possesso, devi bloccare subito la carta e prendere contatto con la banca. Questa ti fornirà tutti i chiarimenti necessari e provvederà ad effettuare le opportune verifiche. In questo caso, la tua carta potrebbe essere stata clonata (vedi a pag. 14).

## IL SERVIZIO FARO

**Cerchi uno sportello Bancomat funzionante?**

**Le banche aderenti a PattiChiari ti offrono il servizio FARO** (Funzionamento Atm Rilevato On-line): con una telefonata gratuita al call center, chiamando dal telefono fisso o dal cellulare il numero 800-00.22.66 **entro pochi secondi puoi trovare, 7 giorni su 7, 24 ore su 24, il Bancomat funzionante più vicino, anche quello della tua banca.**

La stessa ricerca puoi farla anche - dal tuo PC o tramite un cellulare - sul sito di PattiChiari - **[www.pattichiari.it](http://www.pattichiari.it)** - o su quello della tua banca: in questo caso ti verrà anche indicato **il percorso migliore per raggiungerlo a piedi o in auto.**

## Le parole della sicurezza

### *Clonazione delle carte*

La “clonazione” della carta avviene attraverso l’applicazione, ad esempio sugli sportelli Bancomat o nei terminali POS che si usano per i pagamenti nei negozi, di apparecchiature in grado sia di copiare le informazioni contenute nella banda magnetica della carta stessa sia di rilevare il codice PIN inserito dal cliente.

Chi ha raccolto queste informazioni è in grado di “duplicarle” su altro supporto plastico e utilizzarlo per transazioni fraudolente (acquisti e/o prelievi).

### *Phishing*

Il phishing consiste nella creazione e nell’uso di e-mail o sms (smishing) che invitano a consultare siti web realizzati dai frodatori per apparire come se fossero autentici siti della banca, con l’obiettivo di carpire informazioni personali e riservate (ad esempio le password per i servizi di internet banking o il numero di carta di credito). Puoi riconoscere i messaggi di truffa con qualche piccola attenzione: generalmente non sono personalizzati, hanno un tono intimidatorio e chiedono di trasmettere le proprie credenziali fornendo il collegamento al sito sul quale dovrebbero essere inserite.

Non rispondete mai alle e-mail; banche ed enti emittenti non chiedono mai di inviare informazioni su dati personali o delle carte via e-mail. Nel dubbio sempre meglio fare una telefonata.

## *Virus e Spyware*

Con il termine Virus si intende un programma che può diffondersi sui computer e sulle reti creando un duplicato del programma stesso, a tua insaputa. I virus possono alterare il normale funzionamento del tuo PC, provocando effetti più o meno dannosi, che vanno dalla visualizzazione di messaggi fastidiosi sullo schermo alla sottrazione dei tuoi dati riservati, alla cessione ad altri utenti del controllo del tuo computer.

Con il termine Spyware si intende un tipo particolare di virus che consente di raccogliere informazioni sulle abitudini dell'utente. Una delle tipologie più insidiose di virus va sotto il nome di Crimeware. Si tratta di una specifica classe di codici malevoli in grado di reperire autonomamente informazioni personali sui PC infetti e trasmetterle a un potenziale truffatore. L'azione di contrasto inizia quindi già nel momento del tentativo di contagio, che puoi prevenire mantenendo le semplici regole di protezione della tua postazione riportate in questa Guida.

## *Falsi annunci di lavoro*

Il percorso completo della frode non si ferma all'acquisizione illegale dei dati personali dei clienti. I truffatori, con lo scopo di rendere più difficoltosa la tracciabilità e il contrasto delle operazioni criminali, spesso ricorrono alla collaborazione inconsapevole degli stessi clienti delle banche, mediante la diffusione via e-mail di falsi annunci di lavoro. Lauti compensi sono offerti in cambio della disponibilità del proprio conto corrente come appoggio per effettuare movimentazioni di denaro, dando così vita ad un'azione di riciclaggio di denaro, reato perseguibile penalmente.

Iniziativa in collaborazione con:



[www.adiconsum.it](http://www.adiconsum.it)



[www.adoc.org](http://www.adoc.org)



[www.altroconsumo.it](http://www.altroconsumo.it)



[www.assoutenti.it](http://www.assoutenti.it)



[www.casadelconsumatore.it](http://www.casadelconsumatore.it)



[www.cittadinanzattiva.it](http://www.cittadinanzattiva.it)



[www.codacons.it](http://www.codacons.it)



[www.codici.org](http://www.codici.org)



[www.confconsumatori.com](http://www.confconsumatori.com)



Lega Consumatori

[www.legaconsumatori.it](http://www.legaconsumatori.it)



[www.movimentoconsumatori.it](http://www.movimentoconsumatori.it)



[www.mdc.it](http://www.mdc.it)



[www.consumatori.it](http://www.consumatori.it)