Protezione dei dati bancari, la conosci davvero?

Le dieci cose da sapere per proteggere i tuoi dati bancari

DOCUMENTO ACCESSIBILE A IPOVEDENTI E NON VEDENTI*

noi & UniCredit

Documento sviluppato con le Associazioni dei Consumatori partner del Programma Noi&UniCredit

ADICONSUM – Associazione Difesa Consumatori e Ambiente promossa dalla CISL

ADOC – Associazione Difesa Orientamento Consumatori

ASSOUTENTI

Casa del Consumatore

CITTADINANZATTIVA

CODACONS

CONFCONSUMATORI APS

Federconsumatori

LEGA CONSUMATORI

MOVIMENTO CONSUMATORI

MOVIMENTO DIFESA del Cittadino

U.Di.Con. – Unione per la Difesa dei Consumatori

1955 UNC CONSUMATORI.IT

UniCredit

* Accessibile su lettori con lingua italiana conformi agli standard PDF/UA

1 COSA FARE SE SI RICEVE UNA TELEFONATA O UNA MAIL DALLA PROPRIA BANCA IN CUI VENGONO CHIESTE LE CREDENZIALI DI ACCESSO AL PROPRIO CONTO ONLINE?

La banca non contatta mai telefonicamente o via mail i clienti per conoscere codici personali di accesso all'internet banking oppure PIN (Personal Identification Number - numero identificativo personale) o numeri delle carte di pagamento. Nel caso in cui riceviate telefonate da qualcuno che non conoscete e che si presenta come dipendente della vostra banca, se vi venisse richiesto di fornire informazioni o di eseguire pagamenti a titolo di rimborso o per risolvere una situazione di emergenza, chiudete la telefonata e contattate la vostra banca tramite il numero che trovate sul sito o sul retro della carta di pagamento. Qualora invece abbiate ricevuto una mail o messaggi sospetti non cliccate su link, non aprite eventuali allegati, non inserite le credenziali di accesso al conto e non contattate numeri di telefono riportati nelle comunicazioni che non siano effettivamente riconducibili alla banca.

ATTENZIONE
Anche mail e SMS che sembrano provenire dalla banca potrebbero essere fasulli così come telefonate o messaggi provenienti dal numero dal quale la banca vi manda comunicazioni, infatti tramite lo "**spoofing**" (una tipologia di attacco informatico) i truffatori riescono ad ingannare la vittima riproducendo indirizzi mail o numeri di telefono noti. Lo spoofing viene utilizzato anche in combinazione con sistemi di intelligenza artificiale generativa con i quali si riescono ad imitare voci e interagire in modo autentico, senza fornire alcun indizio sulla vera identità di chi sta chiamando. Occorre quindi prestare la massima attenzione alle comunicazioni che si ricevono verificando l'indirizzo di provenienza e, in caso di dubbio, contattare l'assistenza clienti della banca.

2 MEMORIZZARE I DATI DELLE CARTE DI PAGAMENTO SU DISPOSITIVI E SITI ONLINE È SICURO?

Salvare sullo smartphone (ad esempio nella rubrica) i dati o l'immagine delle proprie carte di pagamento o autorizzare siti online o browser web a conservare tali dati sono pratiche utilizzate per velocizzare gli acquisti molto pericolose. È possibile smarrire lo smartphone col rischio di permettere l'accesso a malintenzionati ai dati che abbiamo salvato sullo stesso, soprattutto se lo smartphone non è protetto da codici di accesso o da modalità di riconoscimento biometrico come l'impronta digitale o il riconoscimento facciale. Così come il sito su cui abbiamo salvato i dati potrebbe subire attacchi hacker e, in assenza di adeguati sistemi di protezione, potrebbero essere trafugati e abusivamente diffusi e utilizzati.

ATTENZIONE
Evitare di memorizzare sullo smartphone i dati della carta di pagamento e in generale ogni dato bancario e personale, come PIN, password, ecc.

3 È RISCHIOSO CONSERVARE IL PIN INSIEME ALLA CARTA DI PAGAMENTO?

Il PIN delle carte di pagamento è un dato indispensabile per concludere le operazioni di pagamento è quindi fondamentale gestirlo in sicurezza. Si sconsiglia dunque di conservarlo insieme alla carta o di scriverlo direttamente su di essa, sarebbe come lasciare le chiavi di casa inserite nella toppa della porta quando usciamo.

ATTENZIONE
Per rendere più semplice la memorizzazione del PIN alcune banche consentono di cambiarlo con un codice più familiare. Se optate per questa soluzione è bene evitare di scegliere codici banali come 1234 o simili.

4 COME SCEGLIERE UNA PASSWORD SICURA?

La scelta di una buona password è fondamentale per proteggere la tua sicurezza e la tua privacy. **Il tempo necessario per scoprire una password varia in base al numero di caratteri utilizzati e alla loro combinazione**. Una password di quattro, cinque o sei caratteri anche combinando lettere maiuscole, lettere minuscole, numeri e simboli può essere scoperta, tramite appositi software utilizzati dai truffatori, istantaneamente. Per individuare password più complesse formate da 14 caratteri con lettere maiuscole, lettere minuscole e numeri potrebbero essere necessari anni e, se presenti anche simboli, potrebbero occorrere addirittura secoli.
Per proteggere i propri account si consiglia quindi di **utilizzare password complesse composte da almeno 14 caratteri e comprensive di tutti i tipi di caratteri accettati** (lettere maiuscole, lettere minuscole, numeri e simboli). Le password complesse sono più difficili da ricordare ma anche decisamente più sicure.

ATTENZIONE
Per ricordare le proprie password si può utilizzare la mnemotecnica, per esempio scegliendo una frase facile da ricordare, il titolo del proprio film preferito e sfruttare la prima lettera di ogni parola per ottenere un acronimo da usare come password, magari inserendo anche numeri, simboli e lettere maiuscole non solo come primo carattere. Si consiglia inoltre di **utilizzare password diverse per siti/account diversi**.

5 L'AUTENTICAZIONE CON RICONOSCIMENTO BIOMETRICO È SICURA?

L'autenticazione biometrica tramite l'impronta digitale o il riconoscimento facciale permette di accedere all'app della tua banca e autorizzare le operazioni in sicurezza senza digitare il PIN.

ATTENZIONE
Si tratta di un sistema che garantisce maggiore sicurezza in quanto basato sulle caratteristiche biologiche uniche di ciascuna persona.

6 È UTILE MONITORARE I MOVIMENTI BANCARI E ATTIVARE IL SERVIZIO DI ALERT?

Controllare periodicamente il conto corrente consente di verificare i movimenti e gli addebiti sul conto stesso e sulle carte di pagamento. Può essere utile a tal fine anche impostare un sistema di notifiche per le operazioni più rilevanti per essere informati tempestivamente sui movimenti del conto e, in caso di frode, individuarli e segnalarli alla propria banca immediatamente.

ATTENZIONE
Si consiglia di annotare il numero da contattare per bloccare le proprie carte di pagamento in caso di furto, smarrimento, contraffazione o uso non autorizzato.

7 IL PAGAMENTO CONTACTLESS È SICURO?

La tecnologia contactless, grazie all'utilizzo della tecnologia RFID (Radio Frequency Identification) permette di effettuare pagamenti semplicemente avvicinando la carta di pagamento al POS senza doverla inserire. I pagamenti contactless possono essere effettuati anche tramite smartphone/smartwatch dotati di tecnologia NFC (Near Field Communication).

ATTENZIONE
Per pagamenti fino a 50 euro non è necessario digitare il PIN, che sarà richiesto al raggiungimento della soglia di 150 euro di utilizzo consecutivo della carta senza digitazione del PIN.

8 COME SMALTIRE CORRETTAMENTE LE CARTE DI PAGAMENTO SCADUTE?

Le carte di pagamento scadute possono essere riconsegnate presso le filiali della tua banca che si occuperanno di gestire correttamente il rifiuto oppure, prima di smaltirle presso i centri di raccolta o le isole ecologiche, si consiglia di tagliarle in piccoli pezzi, soprattutto in corrispondenza della banda magnetica e del chip, per evitare che qualcuno si possa appropriare dei dati bancari del titolare.

ATTENZIONE
Il numero presente sulla carta di credito scaduta rimane invariato sulla nuova. Una carta di credito scaduta è inutilizzabile ma contiene i dati bancari del titolare pertanto, per tutelare la sua sicurezza, si consiglia di smaltirla correttamente.

9 UTILIZZARE IL WALLET È SICURO?

Il wallet è un portafoglio digitale che permette di inserire le carte di credito, prepagate e di debito, direttamente sullo smartphone per effettuare pagamenti avvicinando il dispositivo al POS, senza dover utilizzare le carte fisiche.

ATTENZIONE
Le informazioni delle carte **non vengono memorizzate sul dispositivo né trasmesse durante il pagamento** si tratta quindi di un metodo di pagamento che garantisce la sicurezza delle transazioni.

10 L'APP DELLA BANCA VA AGGIORNATA?

L'App della banca permette di gestire in tutta semplicità il proprio conto corrente online offrendo maggiore comodità e immediatezza nell'effettuare le principali operazioni bancarie. Si consiglia quindi di utilizzare l'ultima versione dell'App e di effettuare sempre gli aggiornamenti.

ATTENZIONE
Un'App aggiornata risolve eventuali problemi riscontrati nelle versioni precedenti, permette di usufruire delle ultime funzionalità e migliora la sicurezza del sistema.