

Ecco un promemoria, da stampare e conservare, contenente alcuni consigli utili per la tua sicurezza.

1

NON COMUNICARE IL NUMERO DELLA TUA CARTASI AD ESTRANEI!

Se vieni contattato, via telefono o per posta elettronica, da sconosciuti che dichiarano di lavorare per CartaSi, **NON FORNIRE IL NUMERO DELLA TUA CARTA!** Il nostro personale preposto ai contatti con la Clientela, HA GIÀ TUTTI I TUOI DATI e non ha quindi motivo di chiamarti per chiederti di comunicarli nuovamente!

Chunque ti chiami, o ti contatti, anche via e-mail, chiedendo il numero della tua carta di credito o altri tuoi dati è quindi, molto probabilmente, UN TRUFFATORE.



Se ricevi chiamate o richieste che ti appaiono sospette, segnalalo subito al **Servizio Clienti** di CartaSi al **Numero Verde 800-15.16.16**.

2

E-MAIL: ATTENZIONE AL PHISHING!

Presta molta attenzione all'uso corretto della posta elettronica: si sta purtroppo diffondendo una forma di truffa molto insidiosa nota con il nome inglese di "phishing".

Questa tipologia di truffa sfrutta la richiesta di informazioni "confidenziali" che vengono raccolte attraverso richieste false inviate via e-mail. Le false richieste ti potrebbero giungere con lo scopo di sottrarti, ovviamente a tua insaputa, dati personali e confidenziali (il numero della tua carta di credito, la tua password o altri dati e codici di sicurezza).

I falsi messaggi e-mail, camuffati in modo da assomigliare a quelli provenienti da soggetti affidabili (banche, compagnie di carte di credito o società molto note e attive nel commercio elettronico), inducono i destinatari a fornire - in assoluta buona fede - i propri dati personali, tra cui quelli della carta di credito.

Diffida dalle e-mail che:

- contengono un messaggio generico di richiesta di informazioni personali per motivi non ben specificati (es. scadenza, smarrimento, problemi tecnici)
- fanno uso di toni 'intimidatori', ad esempio minacciando il blocco della carta in caso di mancata risposta dell'utente
- provengono da indirizzi web molto lunghi contenenti caratteri inusuali, quali in particolare '@'



Un esempio di phishing

Al tuo indirizzo di posta elettronica potrebbe arrivare una e-mail che ti segnala la possibilità che qualcuno abbia usato i tuoi dati per fare acquisti on line. Il messaggio ti invita, quindi, a verificare la situazione digitando, nella finestra che si apre in automatico all'apertura della e-mail, il tuo codice di accesso ai servizi dispositivi della carta di credito (nel caso di CartaSi, il Codice Identificativo Personale).

*Dopo aver digitato i dati, appare un messaggio che avverte che si sono verificati problemi di connessione... **a questo punto i tuoi dati sono già nelle mani sbagliate!***

Questo esempio è tratto da uno dei numerosi casi realmente accaduti: se dovessi trovarti in una situazione simile, **NON** rispondere alla mail, **NON** fornire i dati della tua carta di credito e/o altri codici di sicurezza e **AVVISA SEMPRE** tempestivamente **CartaSi**, girando la mail a **Segnalazioni_Phishing@cartasi.it!**

3

CUSTODISCI CON CURA IL TUO PIN!

Il PIN (Personal Identification Number) è un codice riservato che non deve essere reso noto a terze persone: cerca di memorizzarlo, non trascriverlo (neanche sulla rubrica telefonica!) e non conservarlo **mai** insieme alla carta, nel portafoglio o in borsa. In questo modo sarai tutelato contro i prelievi di contante da parte di terzi, per i quali non è previsto alcun rimborso, anche se avvengono a seguito di smarrimento, sottrazione o contraffazione della carta.

4

RITIRA SEMPRE LE RICEVUTE AI SELF SERVICE!

Gli impianti self service che consentono il pagamento con carta di credito (carburanti, parcheggi) rilasciano una ricevuta che riporta i dati della carta (numero e scadenza). **RITIRA SEMPRE LA RICEVUTA**: se cade nelle mani sbagliate puoi rischiare che i dati della tua carta vengano usati per acquisti su Internet!

Aiutaci anche tu a prevenire le frodi!

5

QUANDO FAI ACQUISTI SU INTERNET, USA QUESTE CAUTELE:

- verifica sempre che il "venditore" sia un esercizio reale, meglio se conosciuto, e che il sito indichi tutti i suoi dati, compreso l'indirizzo
- evita di inserire il numero della carta come prova della maggiore età o per qualsiasi altro motivo e, comunque, diffida degli accessi gratuiti a siti che richiedono poi, a vario titolo, i dati della carta di credito
- evita di inserire il numero della tua carta in siti non protetti da sistemi di sicurezza internazionali, riconoscibili dal lucchetto che appare sulla schermata e dal relativo certificato di protezione (per visualizzare il certificato di protezione, clicca due volte sull'icona del lucchetto). All'interno del certificato, il nome visualizzato accanto alla voce "Rilasciato a" deve corrispondere, o quantomeno essere simile, a quello del sito che stai visitando. Se invece il nome è molto diverso, o non sei certo dell'autenticità di un certificato, non inserire i tuoi dati, evita di eseguire qualsiasi operazione e lascia immediatamente il sito!
- prendi sempre nota dell'indirizzo Internet del sito presso il quale hai effettuato l'acquisto
- leggi attentamente le condizioni del servizio offerto ed eventuali clausole contrattuali, tenendo copia cartacea di quanto "sottoscritto virtualmente" inserendo il numero della tua carta
- poni particolare attenzione alle condizioni di pagamento del servizio: spesso il pagamento occasionale è in realtà la sottoscrizione inconsapevole di un abbonamento con ripetuti addebiti mensili!
- diffida di offerte "incredibilmente vantaggiose": se non si tratta di iniziative di aziende note e affidabili, possono nascondere spiacevoli sorprese

6

SE LA TUA CARTASI VIENE RUBATA, O LA SMARRISCI, CHIAMA SUBITO IL SERVIZIO BLOCCHI!

La segnalazione tempestiva del furto o dello smarrimento della tua Carta ne evita l'utilizzo illecito da parte di terzi. Poiché, quando succede, è facile cadere in preda al panico e dimenticare anche il proprio numero di casa, **salva sul tuo cellulare i numeri utili di CartaSi!**



SERVIZIO CLIENTI (attivo 24 ore su 24, 365 giorni all'anno)

dall'Italia: **Numero Verde 800-15.16.16**

dall'estero: **+39-02-3498.0020***

dagli U.S.A.: **Numero Verde internazionale 1-800-473.6896**

**si accettano chiamate a carico di CartaSi*

7

ISCRIVITI AI SERVIZI SMS DI CARTASI!

Se temi di non accorgerti immediatamente del furto o dello smarrimento della tua Carta, o se vuoi garantirti una tutela preventiva contro le frodi, iscriviti ai Servizi SMS di CartaSi: sono **gratuiti** e, fra le altre cose, ti permettono di essere avvisato in tempo reale con un **SMS** di ogni utilizzo della tua Carta superiore ad un importo che tu stesso avrai indicato.

Così, in caso di frode o di spese effettuate con la carta smarrita o sottratta, potrai chiamare il Servizio Clienti e bloccare subito la Carta, evitando l'addebito della/e spesa/e sul tuo conto corrente.

Questa procedura non viene utilizzata in caso di **prelievamenti** avvenuti dagli sportelli automatici con il codice segreto **PIN**: in questi casi, infatti, **non è previsto alcun rimborso**.

8

FIRMA LA TUA CARTASI SUL RETRO!

Quando ricevi la Carta, firmala subito nell'apposito spazio sul retro, sotto la banda magnetica, utilizzando una penna a sfera. Così permetterai all'esercente di verificare la corrispondenza della firma con quella apposta sulla ricevuta d'acquisto e sarai ulteriormente tutelato in caso di utilizzo della tua carta da parte di terzi!

9

PRIMA DI FIRMARE LA RICEVUTA D'ACQUISTO, VERIFICA CHE L'IMPORTO SIA QUELLO DOVUTO

Verifica sempre che l'importo indicato sulla tua ricevuta d'acquisto sia quello corretto e che sia indicato nel campo 'TOTALE'. Alcune ricevute consentono l'indicazione dell'importo 'MANCIA' e vengono quindi compilate dall'esercente solo nel campo 'SUBTOTALE': prima di firmare, indica sempre nel campo 'TOTALE' l'importo del pagamento (con o senza la mancia).

10

CONSERVA LE RICEVUTE D'ACQUISTO FINO ALLA RICEZIONE DELL'ESTRATTO CONTO

Potrai così verificare le tue spese e inviare eventuali richieste di chiarimenti entro il termine previsto dal Regolamento (60 giorni dalla ricezione dell'estratto conto).

11

LA TUA PRIVACY E' SACRA, ANCHE QUANDO PRELEVI AL BANCOMAT!

Tutela la riservatezza delle tue operazioni allo sportello Bancomat!

Diffida di luoghi e situazioni sospetti: gruppi di persone che chiacchierano animatamente e sostano a lungo vicino allo sportello automatico di una Banca non sono un buon segnale.

Non permettere a nessuno di invadere il tuo spazio mentre digiti il PIN. Se qualcuno si avvicina troppo mentre stai compiendo un'operazione, chiedi con fermezza e cortesia che si allontani: il diritto alla Privacy è sacro! Cerca poi di usare sempre la mano libera a protezione dei numeri che stai digitando (questo consiglio vale anche per quando fai un acquisto).

Quando prelevi, ricorda anche che:

- la carta deve poter essere inserita nell'apposita fessura dello sportello **senza sforzo**.
- all'atto della restituzione, la carta deve poter essere facilmente afferrata con le dita senza particolare difficoltà. Se hai sospetti, contatta il personale della banca, le Forze dell'Ordine o, in orari di chiusura degli sportelli, chiama il Servizio Blocchi di CartaSi (o, se stai usando il Bancomat, il Servizio Blocchi Bancomat al Numero Verde 800-822.056) e racconta quanto accaduto: gli operatori ti consiglieranno sul da farsi ed eventualmente provvederanno al blocco cautelativo della tua carta/del Bancomat.
- in caso di mancata restituzione della carta, diffida di sconosciuti disposti ad aiutarti con insistenza e chiama immediatamente e personalmente il Servizio Blocchi!

12

GENERA LE TUE PASSWORD IN MODO NON FACILMENTE INTUIBILE

Una password costituita da frasi o parole facilmente intuibili è una password a rischio.

Ecco dunque qualche suggerimento per creare una password sicura e facilmente memorizzabile:

- crea la tua password componendola con le iniziali di una frase che possa facilmente richiamare alla memoria una situazione familiare soltanto a te e non associabile ai tuoi dati anagrafici. Per maggior chiarezza: QEAIVS (**Q**uesta **E**state **A**ndrò **I**n **V**acanza in **S**ardegna), UMAGLM (**U**na **M**ela **A**i **G**iorno **L**eva il **M**edico), una strofa di una canzone, di una poesia ecc... sono ottimi esempi di password sicure; invece il tuo nome (es. MARIOROSI), la tua data di nascita o quella di un tuo caro sono password facilmente intuibili da truffatori che conoscono il tuo nome o la tua situazione anagrafica
- usa, se possibile, combinazioni di caratteri alfanumerici (QEAIVS0804)
- evita di utilizzare parole di senso comune o riferite alla tua vita privata o aziendale (es. nomi propri, codice fiscale, date di nascita, targa dell'auto, numero del badge personale)