LA SICUREZZA DEI PAGAMENTI VIA INTERNET

Ecco alcune semplici regole e consigli per garantire la sicurezza dei tuoi dati e della tua Carta in internet.
Nexi ti offre la massima tranquillità anche in internet, grazie a servizi e accorgimenti appositamente pensati per garantire la sicurezza non solo della tua Carta - e del suo utilizzo -, ma anche dei tuoi dispositivi.

Proteggi sempre i tuoi dispositivi personali

Se hai un PC, uno smartphone o un Tablet:

- installa e mantieni sempre aggiornato il software di protezione antivirus (i) e anti-spyware;
- installa sempre gli aggiornamenti ufficiali del sistema operativo e dei principali programmi che usi appena vengono rilasciati;
- installa gli aggiornamenti e le patch di sicurezza del browser e delle applicazioni;
- installa un firewall (ii) personale;
- effettua regolarmente scansioni complete con l'antivirus;
- non aprire messaggi di posta elettronica di cui non conosci il mittente o con allegati sospetti;
- non installare applicazioni scaricate da siti non certificati o della cui attendibilità non sei sicuro;
- se lo stesso PC/tablet/smartphone è usato anche da altre persone (familiari, amici, colleghi), fai in modo che adottino le stesse regole;
- proteggi i tuoi dispositivi con PIN, password o altri codici di protezione. Per i consigli su come creare e gestire password e credenziali, ti invitiamo a leggere la sezione dedicata.

(i) *Il software antivirus permette di tenere il proprio dispositivo al riparo da software indesiderati ("malware") che potrebbero essere installati senza il consenso dell'utente, e carpire i dati di pagamento e altri dati sensibili del cliente a scopo fraudolento.*
(ii) *Il firewall personale ha lo scopo di controllare e filtrare tutti i dati in entrata e in uscita del proprio dispositivo, aumentando il livello di sicurezza del dispositivo su cui è installato.*

IMPORTANTE: Nexi non fornisce supporto tecnico su antivirus, firewall e altre soluzioni di sicurezza installati sui dispositivi personali del cliente, né può essere ritenuta responsabile per la configurazione degli stessi.

Password: come crearle e proteggerle

Per motivi di sicurezza l'accesso ad alcune reti o servizi richiede credenziali e password. Queste ultime inoltre vengono utilizzate anche per la protezione di dispostivi personali, per evitare l'accesso a persone non autorizzate. Ecco allora qualche suggerimento per creare - e custodire - una password sicura e facilmente memorizzabile da te, ma non facilmente intuibile da altri:

- crea la tua password - che deve avere obbligatoriamente almeno 8 e massimo 20 caratteri - componendola usando combinazioni di caratteri alfanumerici, di cui almeno una lettera maiuscola. Utilizza ad esempio le iniziali di una frase che possa ricordare soltanto tu e non associabile ai tuoi dati anagrafici. Ad esempio: Qeaivis0804 (Questa Estate Andrò In Vacanza in Sardegna). Il tuo nome (es. MARIO ROSSI), 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;
- non utilizzare password condivise con altri servizi online;
- 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);
- non salvare la password nel browser e evita per quanto possibile di annotarti la password per ricordarla. In ogni caso non conservarla insieme agli strumenti di pagamento;
- non comunicare la password con amici, conoscenti, operatori del Servizio Clienti. Ti ricordiamo che Nexi non ti chiederà mai di comunicare o inviare la tua password né telefonicamente né via mail.

Tutela i tuoi acquisti in internet

Con Nexi puoi utilizzare la tua Carta in tutta tranquillità anche per le tue spese online, grazie al servizio 3D Secure. Con il nome 3D Secure si definisce il sistema di protezione degli acquisti online tramite "Verified by Visa" e "Mastercard SecureCode" studiato dai circuiti internazionali Visa e Mastercard.

Attivare il servizio 3D Secure garantisce una tutela per i tuoi acquisti online, permettendo di prevenire eventuali utilizzi illeciti della tua Carta sul web. Con l'iscrizione al servizio 3D Secure eviti che il tuo numero di Carta venga usato per pagamenti online a tua insaputa. Per attivare il 3D Secure, è necessario essere iscritti al Portale del sito Nexi e avere attivato i Servizi SMS. Il processo di attivazione è facile e veloce: basta impostare la tua frase identificativa e inserire il numero di cellulare registrato ai Servizi SMS.
Durante i tuoi acquisti online, dopo aver inserito i dati richiesti dall'esercente per il pagamento, ti viene mostrata una finestra con la "frase identificativa" da te scelta al momento dell'attivazione del 3D Secure. In questo modo hai la certezza di essere su un sito sicuro certificato 3D Secure.

Al momento del pagamento, se previsto dal sistema, ricevi un SMS da Nexi al numero di cellulare iscritto ai servizi **SMS Alert** con il codice di sicurezza dinamico di 6 cifre, utilizzabile solo una volta, da inserire online per completare l'acquisto. Puoi attivare il 3D Secure su tutte le carte in tuo possesso, anche se ne hai più di una. In questo caso dovrai iscrivere al servizio ogni carta.
Cosa fare in caso di furto/smarrimento dei tuoi dispositivi o delle tue carte o in caso di pagamenti anomali
Se perdi, o ti vengono sottratti, i tuoi dispositivi personali o le tue Carte,o in caso di abuso riscontrato o sospetto (per maggiori dettagli ti invitiamo a leggere anche la sezione dedicata al phishing) è importante agire tempestivamente. In questi casi, contatta immediatamente il Servizio Clienti Nexi (attivo 24 ore su 24) per:

- bloccare immediatamente la tua Carta e le tue credenziali di accesso al Portale del sito Nexi;
- verificare e, nel caso, bloccare eventuali pagamenti sospetti.

Attento al Phishing

Anche in internet, ci sono diversi pericoli. Una truffa molto diffusa è il phishing, una pratica illegale messa in atto da malintenzionati (phisher) che, inviando agli utenti messaggi email rassomiglianti - nei contenuti e nella grafica - a quelli di aziende note, cercano di carpire informazioni riservate e sensibili (codici di accesso, dati della carta di credito o personali) tramite link a siti simili a quelli reali. Nexi è molto attenta ad analizzare la rete con sistemi informatici avanzati, alla ricerca di siti clone che possano creare danno ai Clienti, e segnala gli indirizzi dei siti compromessi ai motori di ricerca.

Ecco alcuni preziosi consigli per capire se ti trovi su un sito phishing o hai ricevuto una mail di phishing:

- **Indirizzo internet contraffatto**
  Come riconoscere quindi un indirizzo potenzialmente pericoloso? La parte iniziale deve essere caratterizzata dalla presenza dell'"https": significa che quel sito utilizza protocolli sicuri per la gestione dei dati personali. Inoltre, l'URL di un sito rimane nel tempo la stessa: il Portale Titolari ha l'indirizzo https://titolari.cartasi.it, il Portale Aziende ha l'indirizzo https://aziende.cartasi.it, perciò devi considerare inaffidabile e pericoloso un sito identico a cui corrisponde un indirizzo diverso
- **Analizza il testo della comunicazione**
  Fai attenzione alle comunicazioni con errori ortografici e grammaticali e con un utilizzo scorretto della lingua italiana, probabilmente sono mail di phishing

Inoltre: un sito sicuro e certificato che adotta i protocolli di sicurezza per la gestione dei dati, riporta sempre nella finestra del browser - in basso a destra o nella barra degli indirizzi - l'icona del lucchetto, che definisce il sito come sicuro. Devi quindi diffidare dei siti che richiedono l'inserimento di dati sensibili (Login o Password, dati della carta di credito o personali) e che non riportano l'icona del lucchetto: i dati inseriti in quella pagina saranno facilmente trafugabili. Se poi vuoi essere sicuro dell'attendibilità del sito, fai doppio click sull'icona del lucchetto: una scheda ti aiuterà a verificare che le credenziali di sicurezza siano effettivamente quelle del sito che stai visitando.

Segnala a Nexi un phishing
Se hai il dubbio di aver lasciato i tuoi dati su un sito contraffatto, Nexi ha creato una casella di posta a cui inoltrare queste segnalazioni. Scrivi all'indirizzo segnalazioni.phishing@cartasi.it, specificando nel testo l'indirizzo del sito e allegando il testo della mail che hai ricevuto.

Nell'area Sicurezza del sito Nexi trovi inoltri i consigli sempre aggiornati su come riconoscere una e-mail o un sito phishing.

Attenzione al Vishing

Il vishing è una forma di phishing basata sull'uso del telefono. Viene richiesto, tramite email o SMS, di chiamare un numero tele- fonico al quale comunicare i propri codici identificativi (Username/Email e Password). In alternativa, viene effettuata

Nexi Payments SpA, sede legale: Corso Sempione, 55 - 20149 Milano Iscritta all'Albo degli Istituti di pagamento art. 114 septies T.U.B. n. 32875.7 Capitale Sociale Euro 56.888.798,40 i.v., Registro delle Imprese di Milano, Codice Fiscale e Partita IVA: 04107060966 REA Milano: 1725898 - Telefono: +39.02.3488.1 Fax: +39.02.3488.4115
Sito Internet: www.nexi.it

LA SICUREZZA DEI PAGAMENTI VIA INTERNET

una chiamata preregistrata, in cui viene chiesta l'immissione e conferma dei codici identificativi. Nexi non ti chiederà mai di comunicare o inserire telefonicamente i tuoi codici identificativi.

Responsabilità di Nexi e del Titolare della Carta per le operazioni in internet
Sia Nexi che il Cliente (Titolare della Carta) devono garantire, ciascuno per la propria parte, l'uso corretto e sicuro dei pagamenti in internet. In particolare, come Cliente, sei responsabile della tua Nexi, e sei tu a dover rispondere legalmente delle operazioni effettuate dai titolari di carte aggiuntive legate alla tua carta.
Devi custodire con cura la tua Carta, il PIN e gli eventuali altri i codici di sicurezza e usarla correttamente. In caso di anomalie o problemi riscontrati durante le operazioni di pagamento in internet, o in caso di abuso o utilizzo sospetto della tua Carta, devi immediatamente contattare il Servizio Clienti Nexi nelle modalità indicate in precedenza. Inoltre, se controllando le spese in estratto conto, ne trovi una che ritieni di non aver fatto o sulla quale vuoi maggiori informazioni, il Servizio Clienti avvierà le eventuali verifiche.

RICORDA: dal momento in cui ricevi l'estratto conto, hai 60 giorni di tempo per inviarci eventuali contestazioni relative alle operazioni addebitate.

Puoi trovare i riferimenti del Servizio Clienti sulla lettera che accompagna la Carta, sull'estratto conto o sul sito Nexi, nella sezione Contatti.

Lato suo, Nexi mette a disposizione della Clientela il Servizio Clienti, disponibile 24 ore su 24, per bloccare la Carta (e quindi il suo utilizzo).