# LA SICUREZZA DEI PAGAMENTI

## Ecco alcune semplici regole e consigli per garantire la sicurezza dei tuoi dati e della tua Carta.

Nexi ti offre la massima tranquillità, 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:**

- installa e mantieni sempre aggiornato il software di protezione antivirus ([1]) e antispyware
- 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
- elimina periodicamente i cookies e i file temporanei Internet utilizzando le opzioni del tuo browser
- installa un firewall ([2]) personale
- effettua regolarmente scansioni complete con l'antivirus
- non installare applicazioni scaricate da siti non certificati o della cui attendibilità non sei sicuro
- se lo stesso PC è usato anche da altre persone (familiari, amici, colleghi), fai in modo che adottino le stesse regole
- proteggi il tuo PC 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.

*([1]) 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.*

*([2]) 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.*

**Se hai uno smartphone o un tablet:**

- installa sempre gli aggiornamenti ufficiali del Sistema operativo appena vengono rilasciati
- installa gli aggiornamenti e le patch di sicurezza di browser e applicazioni
- installa e mantieni aggiornato il software di protezione antivirus e ricorda di disattivare Wi-Fi, geolocalizzazione e bluetooth quando non li usi
- utilizza esclusivamente app ufficiali provenienti da app store affidabili e, in fase di installazione, fai attenzione ai permessi richiesti assicurandoti che siano strettamente connessi al servizio che intendi utilizzare
- proteggi il tuo smartphone o tablet con password, PIN e se possibile con sistemi di riconoscimento biometrico (impronta digitale, riconoscimento del volto, ...). Per i consigli su come creare e gestire password e credenziali, ti invitiamo a leggere la sezione dedicata
- imposta il blocco automatico del tuo dispositivo quando entra in stand-by per proteggere i tuoi dati e, quando possibile, attiva la crittografia del dispositivo e della memory card esterna
- attiva, quando possibile, le funzionalità di "remote lock" e "remote wiping", che ti consentiranno, in caso di furto, di bloccare e cancellare i dati contenuti sul tuo dispositivo mobile da un altro PC

Indipendentemente dal dispositivo che utilizzi, ricorda di non aprire messaggi di posta elettronica di cui non conosci il mittente o con allegati sospetti. Applica le stesse regole alle app di messaggistica istantanea e non aprire allegati o link inviati da utenti sconosciuti.

([1]) **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. MARIOROSSI), 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
- modifica periodicamente la password di accesso alla tua area riservata, soprattutto quando hai ragionevole sospetto che la sua riservatezza possa esser stata violata

## Tutela i tuoi acquisti in internet

Per effettuare in sicurezza acquisti in Internet ricorda di:

- evitare di effettuare transazioni online da computer condivisi o postazioni in luoghi che potrebbero essere poco sicuri, come hotel e cafè
- effettuare il log out dal sito di e-commerce, al termine di ogni acquisto
- utilizzare credenziali diverse per autenticarti su siti diversi ed evita il "salvataggio automatico" delle password sul browser
- valutare sempre l'affidabilità del rivenditore e del sito di e-commerce a cui ti stai rivolgendo. Leggi se possibile eventuali commenti e recensioni lasciate da altri utenti per farti un'idea della controparte commerciale, qualora non la conoscessi

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. L'attivazione del servizio 3D Secure garantisce una tutela per i tuoi acquisti online, permettendo di prevenire eventuali utilizzi illeciti della tua Carta sul web, evitando che il tuo numero di Carta venga usato per pagamenti online a tua insaputa.
Per l'attivazione del 3D Secure, è necessario essere iscritti al Portale del sito Nexi e avere attivato i **Servizi SMS Alert.** 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 servizio dovrà essere attivato su 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 è importante agire tempestivamente. In questi casi, contatta immediatamente il Servizio Clienti Nexi (attivo 24 ore su 24) per:

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

In caso di furto o smarrimento della Carta non dimenticare di rivolgerti alle Forze dell'Ordine per sporgere denuncia.

## Attenti al Phishing

Il phishing è una tipologia di frode informatica che si realizza tipicamente mediante la creazione di siti internet fraudolenti rassomiglianti – nei con tenuti e nella grafica – a quelli di aziende note, cui il Cliente viene invitato a collegarsi tramite invio di false e-mail o sms, convincendolo a fornire informazioni personali, dati finanziari o codici di accesso.
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 identificare un tentativo di phishing:**

- **Controlla l'indirizzo email**
  Fai attenzione all'indirizzo e-mail del mittente. Tipicamente i pirati informatici utilizzano degli indirizzi di posta elettronica che sembrano essere quelli ufficiali, ma in realtà differiscono anche solo di una lettera. (es. mario.rossi@nexii.it). Prima di cliccare su di un link presente in una email, accertati che la e-mail arrivi veramente da un mittente ed un indirizzo ufficiale.
- **Analizza il testo della comunicazione**
  Fai attenzione alle comunicazioni che presentano errori ortografici e grammaticali o fanno un uso scorretto della lingua italiana, probabilmente sono mail di phishing. Diffida da mail contenenti messaggi con toni intimidatori e con carattere d'urgenza che ti chiedono la verifica di dati per s-onali o di Carta di Credito. Sappi che Nexi, per politiche di antiphishing, non chiederà in nessun caso di verificare i tuoi dati anagrafici e/o numeri di carta di credito contattandoti via email o accedendo a pagina web per il suddetto motivo.
- **Controlla l'indirizzo del sito internet**
  Per connetterti al sito di Nexi, digita direttamente l'indirizzo nella barra di navigazione e controlla di aver scritto correttamente il nome del sito. Evita di cliccare su link che rimandano al sito della banca se all'interno di email o SMS sospetti. Le email di phishing fanno inoltre uso di URL abbreviate (short URL) per nascondere indirizzi web non legittimi. Non aprire mai short URL sospette.
  Verifica che il sito web a cui accedi sia caratterizzato dalla presenza dell'"https", a garanzia dell'utilizzo di protocolli sicuri di comunicazione e che sia emesso su un dominio di proprietà di Nexi. Verifica che sia presente il lucchetto verde nel browser, cioè che il sito sia certificato e sicuro. ([3])

*(3) Un sito sicuro e certificato adotta i protocolli di sicurezza per la gestione dei dati, assicura l'integrità dei dati e garantisce comunicazioni cifrate tra il tuo dispositivo e il servizio a cui ti connetti.*

**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@nexi.it, specificando nel testo l'indirizzo del sito e allegando il testo della mail che hai ricevuto.

Nell'area Sicurezza del sito Nexi trovi inoltre 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 telefonico al quale comunicare i propri codici identificativi (Username/Email e Password). In alternativa, viene effettuata 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.

## Ulteriori Consigli di Sicurezza

Infine:

- Pensaci prima di allegare alle email o inviare per altri canali immagini relative ai tuoi strumenti di pagamento, valutando attentamente motivazioni e destinatari
- Verifica la provenienza di buoni acquisto ottenuti online e l'affidabilità dell'esercente, prima di fornire qualsiasi informazione personale.

## 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 Carta, 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 (mai insieme con la Carta!) 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. Controlla regolarmente le movimentazioni del conto corrente e l'estratto conto, se controllando le spese, 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 comunque contestare eventuali operazioni non autorizzate o non correttamente eseguite nei termini ed alle condizioni previste dalle disposizioni vigenti. 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 un numero dedicato, disponibile 24 ore su 24, per bloccare la Carta (e quindi il suo utilizzo).