

LA SICUREZZA DEI PAGAMENTI

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, 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 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 dispositivi non modificati, che mantengono le impostazioni e le restrizioni originali del produttore. L'utilizzo di dispositivi jailbroken o rooted potrebbe compromettere la sicurezza del sistema, esponendo a potenziali vulnerabilità e accessi non autorizzati;
- 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;
- se lo stesso tablet/smartphone è usato anche da altre persone (familiari, amici, colleghi), fai in modo che adottino le stesse regole
- attiva, quando possibile, le funzionalità di "remote lock" e "remote wiping", che ti consentono, 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.

IMPORTANTE: Nexi o la Banca non forniscono supporto tecnico su antivirus, firewall e altre soluzioni di sicurezza installati sui dispositivi personali del cliente, né possono essere ritenute responsabili 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 dispositivi 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 una lunghezza di almeno 10 caratteri e massimo 128 – componendola utilizzando non più di due caratteri consecutivi uguali in una riga e potenzialmente contenente tutti i caratteri della tastiera, spazio compreso, e facendo attenzione alle maiuscole e minuscole (case sensitive)
- la password deve contenere obbligatoriamente
 - i) almeno una lettera maiuscola (A-Z)
 - ii) almeno una lettera minuscola (a-z)
 - iii) almeno un numero (0-9)
- la password non deve essere riconducibile all'utente (no nome, cognome, data di nascita) e non deve appartenere ad una blacklist contenente valori noti per essere comunemente usati, attesi o compromessi. La blacklist, ad esempio, può contenere, senza pretesa di essere esaustivi: password prelevate da precedenti breach; parole del dizionario; caratteri sequenziali o ripetitivi (ad esempio aaaaaa, 1234abcd, qwerty, ecc.)
- evita di riutilizzare la stessa password su più servizi online;
- crea password senza riferimenti a dati personali o aziendali facilmente intuibili, come nomi, codici fiscali, date di nascita, targhe o numeri di badge;
- evita di annotare la password su supporti facilmente accessibili e non conservarla mai insieme ad altri strumenti di pagamento;
- non comunicare la password a nessuno. Ti ricordiamo che la Banca e Nexi non ti chiederanno mai di comunicare o inviare la tua password, né telefonicamente, né via e-mail, né via SMS;
- modifica periodicamente la password di accesso all'Area Personale.

Sicurezza negli acquisti online

Per effettuare in sicurezza acquisti o prenotazioni in Internet ricorda di:

- evitare di eseguire transazioni online da computer condivisi o da postazioni in luoghi potenzialmente non sicuri, come hotel e caffè;
- eseguire il log out dall'area personale del sito e-commerce al termine dell'acquisto;
- utilizzare credenziali di autenticazione differenti per ciascun sito. Per garantire un adeguato livello di sicurezza delle credenziali, è consigliato l'utilizzo di un password manager affidabile, sia dedicato sia integrato nel browser. ;
- valutare sempre l'affidabilità del rivenditore e del sito di e-commerce, consultando, quando possibile, commenti e recensioni di altri utenti.
- Qualora un acquisto o una prenotazione avvengano tramite link, assicurati che questa modalità sia stata concordata con l'Esercente e; una volta aperto il link, verifica attentamente i dati dell'operazione.

Servizio di protezione Anti-frode 3D Secure

Il Servizio 3D Secure è il sistema di protezione degli acquisti online gratuito studiato dai circuiti internazionali Visa e Mastercard che ti consente di utilizzare la tua Carta in tutta tranquillità per le tue spese online. Il servizio permette di prevenire eventuali illeciti della tua Carta sul web, evitando che il tuo numero di Carta venga usato per pagamenti online a tua insaputa.

L'Emittente si riserva la facoltà di iscrivere di iniziativa e gratuitamente al 3D Secure i Titolari che abbiano comunicato il numero di cellulare a Nexi o tramite la Banca Emittente/ Collocatrice.

Puoi attivare il servizio 3D Secure inserendo il tuo numero di cellulare, ove non già fornito, sull'area Titolari Nexi raggiungibile tramite link, se reso disponibile in Area Personale illimity.

Nei tuoi acquisti online, dopo aver inserito i dati richiesti dall'Esercente per il pagamento, ti verrà mostrata una finestra per completare l'acquisto tramite autenticazione forte, ove prevista dal sistema. Al momento del pagamento, se previsto dal sistema:

1. se sei registrato all'App Nexi Pay, ricevi una notifica autorizzativa e completi l'acquisto online:
 - tramite impronta digitale o riconoscimento facciale su device abilitati al riconoscimento biometrico, oppure
 - inserendo sul sito dell'esercente il codice di sicurezza dinamico di 6 cifre, utilizzabile solo una volta.
2. se non sei registrato all'App Nexi Pay, ricevi un SMS da Nexi al numero di cellulare registrato contenente il codice di sicurezza dinamico di 6 cifre, utilizzabile solo una volta, da inserire online per completare l'acquisto.

Cosa fare in caso di furto/smarrimento dei tuoi dispositivi o della tua Carta o in caso di pagamenti anomali

Se perdi, o ti vengono sottratti i tuoi dispositivi personali o la tua Carta, 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 e/o, 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.

Phishing e altre forme di frode

Il phishing è una forma di frode informatica che si manifesta generalmente attraverso la creazione di siti web fraudolenti che imitano, nei contenuti e nella grafica, quelli di Nexi, delle Banche o di aziende note. Il Cliente viene indotto a collegarsi a tali siti tramite l'invio di e-mail ingannevoli con l'obiettivo di carpire informazioni personali, dati finanziari o credenziali di accesso.

Nexi monitora costantemente la rete mediante sistemi informatici avanzati, al fine di individuare eventuali siti cloni che possano arrecare danno ai Clienti, e provvede a segnalare tempestivamente gli indirizzi dei siti compromessi ai motori di ricerca.

Ecco alcuni preziosi consigli per identificare un tentativo di phishing:

• Controlla l'indirizzo e-mail

Presta 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

Diffida dalle comunicazioni che presentano errori ortografici e grammaticali o fanno un uso scorretto della lingua italiana, probabilmente sono e-mail di phishing. Diffida da mail contenenti messaggi con toni intimidatori e con carattere d'urgenza che ti chiedono la verifica di dati personali o di Carta. Sappi che Nexi, per politiche di antiphishing, non chiederà in nessun caso di verificare i tuoi dati anagrafici e/o numeri di Carta contattandoti via e-mail o accedendo a pagine web.

• 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 e-mail o SMS sospetti. Le e-mail 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 del protocollo "https", a garanzia dell'utilizzo di protocolli sicuri di comunicazione e che sia emesso su un dominio di proprietà di Nexi. Verifica eventuali errori o piccole modifiche nell'URL (ad esempio "niexi.it"), che possono indicare un sito fraudolento, creato appositamente per ingannare l'utente e rubare informazioni personali o credenziali.(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.

Esistono varie tecniche di "social engineering" finalizzate al furto di informazioni o credenziali di accesso, tra cui:

- **Smishing:** invio di SMS ingannevoli con l'obiettivo di convincere l'utente a cliccare link malevoli o a fornire informazioni riservate, come password o codici OTP.
- **Callback phishing:** consiste nell'invio di e-mail o SMS che invitano l'utente a contattare un numero telefonico, gestito da un attaccante: una volta effettuata la chiamata, l'attaccante si finge Nexi o un ente affidabile per ottenere credenziali di accesso e informazioni riservate o convincere la vittima a installare un software dannoso.
- **Spoofting del numero:** consiste nella falsificazione del numero di telefono che appare sul display del destinatario della chiamata. L'attaccante è in grado di manipolare il numero visualizzato sul dispositivo del destinatario, in modo che sembri appartenere a un soggetto legittimo (ad esempio Nexi o un ente affidabile) per ottenere credenziali di accesso e informazioni riservate.
- **Quishing (frode tramite codice QR):** tecnica di attacco che sfrutta codici QR apparentemente innocui che, una volta scansionati, reindirizzano a pagine fraudolente o avviano il download di applicazioni e/o file malevoli, compromettendo la sicurezza del dispositivo.
- **Vishing:** è il phishing via telefono, dove l'attaccante chiama direttamente la vittima fingendosi Nexi o un ente affidabile per ottenere credenziali di accesso o informazioni riservate. In alternativa, viene effettuata una chiamata preregistrata, in cui viene chiesto di comunicare credenziali di accesso.
- **Emotional scam:** truffa in cui l'attaccante inventa una storia convincente (ad esempio, "un parente è in ospedale e ha bisogno di soldi subito") per ottenere denaro, spesso richiedendo azioni immediate come ricariche di carte prepagate.
- **Fake offers:** annunci online o telefonici che propongono prodotti a prezzo incredibile, ma servono solo a ottenere denaro o dati della carta.

Segnala a Nexi un phishing

Se hai il sospetto di aver fornito credenziali personali o dati della carta su un sito contraffatto, invia una mail a segnalazioni.phishing@nexi.it, specificando l'URL del sito e allegando l'e-mail ricevuta.

Nell'area Sicurezza del sito internet Nexi trovi inoltre i consigli sempre aggiornati su come riconoscere una e-mail, un SMS o un sito di phishing.

Nessun dipendente di Nexi chiederà mai di fornire credenziali di accesso tramite e-mail, SMS, telefono o altri canali esterni.

Ulteriori Consigli di Sicurezza

Infine:

- Pensaci prima di allegare alle e-mail 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, sia la Banca sia 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, sul sito Nexi e nell'Area Personale.

È offerta alla Clientela la possibilità di bloccare la Carta in autonomia contattando il numero dedicato, disponibile 24 ore su 24.