LA SICUREZZA DEI PAGAMENTI

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

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 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
- 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 e la Banca non forniscono 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. In particolare, per l'accesso al sito illimity di seguito è riportato 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 al case-sensitive
- 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 aaaaaaa, 1234abcd, qwerty, ecc.)
- evita inoltre parole legate al contesto, ad esempio nome, cognome, nome del servizio, o derivati di queste
- non utilizzare password condivise con altri servizi online
- 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 o la Banca non ti chiederanno mai di comunicare o inviare la tua password né telefonicamente né via mail

Tutela i tuoi acquisti in internet

Il Servizio 3D Secure è il sistema gratuito studiato dai circuiti internazionali Visa e Mastercard con l'obiettivo di incrementare il livello di protezione degli acquisti online. Il servizio mira a prevenire eventuali illeciti della tua Carta sul web (ciò che accade, ad esempio, nei casi in cui il tuo numero di Carta venga usato per pagamenti online a tua insaputa).
Nexi si riserva la facoltà di iscrivere di iniziativa e gratuitamente al 3D Secure i Titolari che abbiano comunicato il numero di cellulare a Nexi anche tramite la Banca.

Puoi attivare il servizio 3D Secure inserendo il tuo numero di cellulare, ove non già fornito, sull'area Personale del Portale o dall'App.

Durante i 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, 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, 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 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 numero del Servizio Clienti Nexi dedicato al blocco della Carta (attivo 24 ore su 24) per:
- bloccare immediatamente la tua Carta
- verificare e, nel caso, bloccare eventuali pagamenti sospetti

Attenti al Phishing

Il phishing è una tipologia di frode informatica che si realizza tipicamente mediante la creazione di siti internet fraudolenti rassomiglianti – nei contenuti 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.
La Banca o Nexi potrebbero segnalare 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@nexi.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 personali o della Carta. Sappi che Nexi e la Banca, per politiche di antiphishing, non chiederanno in

nessun caso di verificare i tuoi dati anagrafici e/o numeri di carta contattandoti via email o accedendo a pagina web per il suddetto motivo.

- **Controlla l'indirizzo del sito internet**

Verificare che il sito web a cui si accede sia caratterizzato dalla presenza dell'"https", a garanzia dell'utilizzo di protocolli sicuri di comunicazione. Verifica che il certificato abbiamo il lucchetto verde e sia stato emesso su un dominio di proprietà di Nexi o della Banca. Controllare sempre che l'URL riportata nel vostro browser corrisponda a quella del sito web che si intende visitare. Le email di phishing fanno inoltre uso di URL abbreviate (*short URL*) per nascondere indirizzi web non legittimi. Non aprire mai short URL sospette.
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, 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 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 o la Banca non ti chiederanno mai di comunicare o inserire telefonicamente i tuoi codici identificativi.

Responsabilità di Nexi, della Banca e del Titolare della Carta per le operazioni in internet

Sia Nexi che la Banca 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 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 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 i dati della rendicontazione, 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, sulla documentazione di rendicontazione periodica o sul Sito illimity, nella sezione Contatti.
Nexi mette a disposizione della Clientela un numero del proprio Servizio Clienti, disponibile 24 ore su 24, dedicato al blocco della Carta (e quindi il suo utilizzo).