LA SICUREZZA DEI PAGAMENTI

Alcune importanti regole e consigli per garantire la sicurezza dei dati del Titolare e della Carta

L'Emittente implementa servizi e accorgimenti appositamente pensati per garantire la sicurezza della Carta, del suo utilizzo e dei dispositivi.

I dispositivi personali sono sempre da proteggere

Personal Computer:

- installare e mantenere sempre aggiornato il software di protezione antivirus ([1]) e antispyware;
- installare sempre gli aggiornamenti ufficiali del Sistema Operativo e dei principali programmi appena vengono rilasciati;
- installare gli aggiornamenti e le patch di sicurezza del browser e delle applicazioni;
- eliminare periodicamente i cookies e i file temporanei Internet utilizzando le opzioni del browser;
- installare un firewall ([2]) personale;
- effettuare regolarmente scansioni complete con l'antivirus;
- non installare applicazioni scaricate da Siti non certificati o della cui attendibilità non si è sicuri;
- se lo stesso PC è usato da più persone, è necessario che tutti adottino le stesse regole;
- il PC va protetto con PIN, password o altri codici di protezione, per i consigli su come creare e gestire password e credenziali, leggere la sezione sotto riportata: "Password: come crearle e proteggerle".

([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.

Smartphone e Tablet:

- installare sempre gli aggiornamenti ufficiali del Sistema Operativo appena vengono rilasciati;
- installare gli aggiornamenti e le patch di sicurezza di browser e applicazioni;
- installare e mantenere aggiornato il software di protezione antivirus e disattivare Wi-Fi, geolocalizzazione e bluetooth quando non in uso;
- utilizzare 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;
- utilizzare esclusivamente app ufficiali provenienti da app store affidabili e, in fase di installazione, prestare attenzione ai permessi richiesti che devono essere strettamente connessi al servizio offerto;
- smartphone e tablet vanno protetti 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, leggere la sezione sotto riportata: Password: come crearle e proteggerle;
- impostare il blocco automatico del dispositivo quando entra in stand-by per proteggere i dati e, quando possibile, attivare la crittografia del dispositivo e della memoria esterna utilizzata (es. SD);
- attivare, quando possibile, le funzionalità di "remote lock" e "remote wiping", che consentono, in caso di furto, di bloccare e cancellare i dati contenuti sul dispositivo mobile da un altro PC.

Indipendentemente dal dispositivo utilizzato, non aprire messaggi di posta elettronica di cui non si conosce il mittente o con allegati sospetti. Applicare le stesse regole alle app di messaggistica istantanea e non aprire allegati o link inviati da utenti sconosciuti.

IMPORTANTE: L'Emittente non fornisce supporto tecnico su antivirus, firewall e altre soluzioni di sicurezza installati sui dispositivi personali del Cliente, né è 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 inoltre vengono utilizzate anche per la protezione di dispostivi personali, per evitare l'accesso a persone non autorizzate. Qualche suggerimento per creare – e custodire – una password sicura e facilmente memorizzabile, ma non facilmente intuibile da altri:

- creare una password lunga da 8 a 20 caratteri, combinando lettere, numeri e almeno una lettera maiuscola; un metodo efficace consiste nell'usare le iniziali di una frase facile da ricordare ma non collegata ai propri dati personali, ad esempio Qeaivis0804 ? "Questa Estate Andrò In Vacanza in Sardegna. Evitare password facilmente intuibili, come il proprio nome (MARIOROSSI) o la data di nascita propria o dei familiari, poiché possono essere facilmente individuate da truffatori che conoscono informazioni anagrafiche;
- evitare di riutilizzare la stessa password su più servizi online;
- creare password senza riferimenti a dati personali o aziendali facilmente intuibili, come nomi, codici fiscali, date di nascita, targhe o numeri di badge;
- evitare di annotare la password su supporti facilmente accessibili e non conservarla mai insieme ad altri strumenti di pagamento;
- non comunicare la password a nessuno. L'Emittente non richiederà mai la password, né telefonicamente, né via e-mail, né via SMS;
- modificare periodicamente la password di accesso all'Area Personale.

Sicurezza negli acquisti online

Per effettuare in sicurezza acquisti o prenotazioni in Internet è necessario:

- evitare di eseguire transazioni online da computer condivisi o da postazioni in luoghi potenzialmente non sicuri, come hotel o 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, assicurarsi che questa modalità sia stata concordata con l'Esercente e, una volta aperto il link, verificare attentamente i dati dell'operazione.

LA SICUREZZA DEI PAGAMENTI

Alcune importanti regole e consigli per garantire la sicurezza dei dati del Titolare e della Carta

Servizio di protezione Anti-frode 3D Secure
Negli acquisti online, dopo aver inserito i dati richiesti dall'Esercente per il pagamento, viene mostrata una finestra per completare l'acquisto tramite Autenticazione Forte, quando prevista dal sistema.
Al momento del pagamento:

1 se si è registrati all'App ed è stata impostata la modalità di accesso con impronta digitale/scansione del viso, si riceve una notifica autorizzativa e si completa l'acquisto online con riconoscimento biometrico;
2 se si è registrati all'App ma non è stata impostata la modalità di accesso con impronta digitale/scansione del viso, o questa non fosse momentaneamente disponibile, si riceve una notifica autorizzativa e si completa l'acquisto inserendo il codice segreto Key6 nell'App;
3 se non si è registrati all'App si inseriscono, nella pagina di pagamento, il codice segreto Key6 ed il codice di sicurezza OTP di 6 cifre collegato dinamicamente alla transazione, che si riceve via SMS da Nexi sul numero di cellulare registrato.

Nexi Key6
Nexi Key6 è il codice a 6 cifre che consente di aumentare il livello di sicurezza degli acquisti online.
Semplice da creare e utilizzare, il codice Key6, inserito direttamente nell'App Nexi Pay oppure digitato insieme al codice ricevuto via SMS nella pagina di pagamento al momento dell'acquisto, è una soluzione efficace per aumentare la sicurezza degli acquisti online. Il codice personale Key6 può essere creato in pochi passaggi dall'Area Personale di Nexi.it o dall'App Nexi Pay.
È inoltre sempre possibile visualizzare, modificare e sbloccare il codice dall'Area Personale su Nexi.it o dall'App Nexi Pay, accedendo alla sezione "Gestisci Carta".

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

In caso di perdita o di sottrazione dei dispositivi personali o della Carta, o in caso di abuso riscontrato o sospetto è importante agire tempestivamente.
In questi casi, è necessario contattare immediatamente il Servizio Blocco Carta (attivo 24 ore su 24) per:

- bloccare immediatamente la Carta e/o le credenziali di accesso all'Area Personale;
- verificare e, nel caso, contestare eventuali pagamenti non autorizzati.

In caso di furto o smarrimento della Carta è necessario rivolgersi 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.
L'Emittente 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.

Alcuni preziosi consigli per identificare un tentativo di phishing:

- **Controllare l'indirizzo email**
  Prestare 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. Prima di cliccare su di un link presente in una e-mail, verificare che la e-mail arrivi veramente da un mittente ed un indirizzo ufficiale.
- **Analizzare il testo della comunicazione**
  Diffidare di comunicazioni che presentano errori ortografici e grammaticali o fanno un uso scorretto della lingua italiana, probabilmente sono e-mail di phishing.
  Diffidare di e-mail contenenti messaggi con toni intimidatori e con carattere d'urgenza che chiedono la verifica di dati personali o della Carta. Per politiche di antiphishing, non sarà richiesto in nessun caso di verificare i dati della Carta o le credenziali personali via e-mail o accedendo a pagine web.
- **Controllare l'indirizzo del Sito Internet**
  Per connettersi al Sito Internet, digitare direttamente l'indirizzo nella barra di navigazione e controllare di aver scritto correttamente il nome del Sito. Evitare di cliccare su link che rimandano al Sito di Nexi e/o 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.
  Verificare che il Sito Web a cui si accede 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 dell'Emittente. Verificare 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)

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.
- **Spoofing 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.

(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 ci si connette.

Come segnalare a Nexi un phishing
Se si sospetta di aver fornito credenziali personali o dati della carta su un sito contraffatto, inviare una mail a segnalazioni.phishing@nexi.it, specificando l'URL del sito e allegando l'e-mail ricevuta.

LA SICUREZZA DEI PAGAMENTI

Alcune importanti regole e consigli per garantire la sicurezza dei dati del Titolare e della Carta

Nell'area Sicurezza del Sito Internet si trovano 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.

Consigli di Sicurezza

E' necessario:

- Pensare prima di allegare alle e-mail o inviare per altri canali immagini relative agli strumenti di pagamento, valutando attentamente motivazioni e destinatari.
- Verificare la provenienza di buoni acquisto ottenuti online e l'affidabilità dell'Esercente, prima di fornire qualsiasi informazione personale.

Responsabilità dell'Emittente e del Titolare della Carta per le Operazioni

Sia l'Emittente, che il Cliente (Titolare della Carta) devono garantire, ciascuno per la propria parte, l'uso corretto e sicuro dei pagamenti in internet. In particolare, il Cliente è responsabile della Carta, e deve rispondere legalmente delle Operazioni effettuate.

La Carta, il PIN e gli eventuali codici di sicurezza vanno custoditi con cura (mai insieme alla Carta!) e vanno usati correttamente.
In caso di anomalie o problemi riscontrati durante le Operazioni di pagamento in internet, o in caso di abuso o utilizzo sospetto della Carta, è necessario contattare immediatamente il Servizio Blocco Carta Nexi con le modalità indicate in precedenza. E' necessario controllare regolarmente le movimentazioni del Conto, e se vi sono spese che si ritiene di non aver eseguito o per le quali si vogliano maggiori informazioni, il Servizio Clienti avvierà le eventuali verifiche.

Si ricorda al Cliente che dal momento dell'addebito (che in caso di carte di credito coincide con l'addebito in conto corrente, mentre in caso di carte prepagate e di debito coincide con la data dell'operazione), ci sono 13 mesi per l'invio di eventuali contestazioni per operazioni non autorizzate o non correttamente eseguite. E' possibile contestare eventuali Operazioni non autorizzate o non correttamente eseguite nei termini ed alle condizioni previste dalle disposizioni vigenti. I riferimenti del Servizio Clienti si trovano sulla lettera che accompagna la Carta, sul Sito Nexi e nell'Area Personale.

E' offerta alla Clientela la possibilità di bloccare la Carta in autonomia tramite l'Area Personale dell'app Nexi Pay (*) o del Portale, nonché mediante il servizio chat con operatore o contattando il numero dedicato, disponibile 24 ore su 24.

(*) Il blocco della carta tramite app Nexi Pay o portale è possibile solo in caso di furto o smarrimento.