LA SICUREZZA DEI DATI

Ecco alcune semplici regole e consigli per garantire la sicurezza dei dati dei tuoi Clienti e del tuo Business.

Proteggi i dati sensibili dei tuoi Clienti e i dati del tuo Business: Nexi ti suggerisce una serie di accorgimenti per garantire la sicurezza dei dati trattati e avere una gestione sicura ed efficiente delle transazioni commerciali che compi ogni giorno.

Proteggi i dati dei tuoi Clienti

Per garantire la massima protezione ai tuoi clienti ed ai loro dati di pagamento devi rispettare una serie di accorgimenti ed adottare una serie di precauzioni che ti aiuteranno ad evitare frodi e compromissione dei dati trattati, sia che la tua attività si svolga in un punto vendita o che il tuo business si svolga prevalentemente online.

Comprendi quali dati stai trattando.
I dati dei Clienti da proteggere sono quelli relativi a:
- transazioni effettuate presso il tuo esercizio commerciale
- dati di carta (nome, cognome, PAN, data scadenza, codice di sicurezza CVV, dati presenti su chip e/o banda magnetica sulla carta).

Non memorizzare mai i dati relativi ai clienti e se strettamente necessario, rendi illeggibili tali dati utilizzando tecniche crittografiche per i dati elettronici. In ogni caso, è preferibile affidare tali attività a terze parti certificate PCI-DSS.
Non inviare mai per email dati di transazioni commerciali o dati di carta di clienti. Le email non sono un mezzo sicuro e soprattutto gli attori operanti nel settore non richiedono mai tali informazioni attraverso email.

Proteggi la tua rete internet

Se nella tua attività commerciale utilizzi una rete WiFi:
- cambia il nome di default della rete Wi-Fi
- modifica le credenziali di default per accedere al pannello di controllo e gestione del router
- controlla che le impostazioni di sicurezza siano quelle desiderate, prestando attenzione a disattivare la gestione remota del router
- imposta una password sicura per accedere alla rete. Per i consigli su come creare e gestire password e credenziali, ti invitiamo a leggere la sezione dedicata
- utilizza password differenti per accesso alla rete e ai tuoi dispositivi e non salvarle mai sul tuo dispositivo
- effettua periodicamente test di sicurezza della tua rete in modo da individuare e risolvere tempestivamente eventuali vulnerabilità presenti. Conserva i report derivanti da tali verifiche

Se nel tuo esercizio commerciale metti a disposizione dei tuoi clienti una rete Wi-Fi ricordati di mantenere segregata tale rete da quella a cui sono collegati POS e dispositivi nel quale memorizzi i dati delle transazioni e dei clienti.

Proteggi sempre i tuoi dispositivi personali

Se nella tua attività commerciale utilizzi un PC:
- installa e mantieni sempre aggiornato il software di protezione antivirus[1] e antispyware
- installa tempestivamente gli aggiornamenti e patch ufficiali del Sistema Operativo e dei principali programmi che usi
- elimina periodicamente i cookies e i file temporanei Internet utilizzando le opzioni del tuo browser
- installa un firewall 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 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.

Se nella tua attività commerciale fai uso di smartphone o tablet:
- installa sempre aggiornamenti del Sistema operativo e delle app appena vengono rilasciati
- 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

Proteggi i tuoi POS

Se utilizzi POS per il pagamento dei clienti, devi custodirli ed avere cura degli stessi in modo da evitare interruzioni di operatività e ridurre il rischio di frodi. Ecco una serie di accorgimenti:

- mantieni un elenco aggiornato dei dispositivi POS che vengono utilizzati nel tuo esercizio commerciale con tutte le relative informazioni (modello, fornitore, numero di serie, ...) in modo da poter individuare rapidamente eventuali smarrimenti
- scatta delle fotografie all'installazione di nuovi terminali POS e conservale per verificare nel tempo la permanenza delle caratteristiche iniziali
- proteggi l'accesso alle funzionalità di configurazione e amministrazione utilizzando password sicure per l'accesso e non utilizzando mai password di default. Per i consigli su come creare e gestire password e credenziali, ti invitiamo a leggere la sezione dedicata
- controlla regolarmente i POS e verifica che non siano presenti tentativi di manomissione (tampering), graffi e segni vicino i bordi e accanto al display e verifica l'integrità dei sigilli presenti su ogni singolo POS
- quando non in uso, riponi i POS in posizioni sicure e controllate. Verifica eventuali posizionamenti in posti diversi e fai in modo che siano chiusi a chiave quando l'esercizio commerciale è chiuso
- verifica che cavi di connessione e connettori, siano dello stesso colore, tipo e numero di quelli installati originariamente e diffida da differenti disposizioni degli stessi
- effettua periodicamente dei controlli di sicurezza su tutti i componenti di cablaggio collegati a POS, registratori di cassa e rete internet per scongiurare la presenza di dispositivi esterni tipo keylogger
- verifica la presenza di dispositivi esterni (e.g. skimmer, pellicole sul tastierino) aggiunti ai POS per scopi fraudolenti
- fai in modo che le aree di pagamento siano ben illuminate e se possibile adotta sistemi di videosorveglianza per monitorarle, prestando attenzione a non permettere la registrazione dei PIN inseriti dai clienti
- effettua manutenzione periodica da fornitori certificati PCI

In caso devi sostituire un POS, accertati che tutti i dati presenti al suo interno siano stati efficacemente cancellati e non più recuperabili.

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, nome dell'esercizio commerciale)
- 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 (almeno una volta ogni 3 mesi) la password di accesso alla tua area riservata, soprattutto quando hai ragionevole sospetto che la sua riservatezza possa esser stata violata

Se ritieni che sia necessario, ricorri a soluzioni di "Autenticazione a due fattori" per rendere più sicuro l'accesso a dispositivi e applicazioni commerciali.

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 l'utente viene invitato a collegarsi tramite invio di false e-mail o sms, convincendolo a fornire informazioni personali, dati finanziari o codici di accesso.

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 personali o di Carta di Credito.
- **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. ([2])

([2]) 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.

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 co m-unicare 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

Per essere sicuro nell'accettazione delle Carte di pagamento ed evitare dispiaceri basta seguire una serie di semplici indicazioni:

- diffida di persone che spendono somme importanti, acquistando in modo frettoloso o in prossimità degli orari di chiusura, o che acquistano più articoli dello stesso tipo o che chiedono di frazionare l'importo
- presta attenzione ad acquirenti che presentano più carte di credito per uno stesso pagamento o che vogliono fare ulteriori acquisti subito dopo averne concluso uno, se senza apparente motivazione
- controlla che sia sempre presente la firma sul retro della Carta, anche se il cliente mostra un documento d'identità, e che corrisponda a quella apposta sul documento di vendita
- controlla sempre l'aspetto della carta: i numeri stampati devono avere un aspetto ordinato e non devono essere in rilievo. Se hai dubbi chiedi l'autorizzazione al Servizio Clienti
- Se l'ordine di pagamento viene compilato manualmente, utilizza l'imprinter, ricorda che non sono validi ordini di pagamento con i dati di Carta compilati manualmente. Nella compilazione dei dati d'acquisto scrivi in maniera leggibile utilizzando una penna
- Richiedi sempre l'autorizzazione al Servizio Clienti se il pagamento non avviene tramite POS e l'importo è superiore al limite di spesa assegnato al tuo punto vendita
- Forma adeguatamente i tuoi collaboratori a porre le stesse cautele nell'accettazione delle Carte. Accurate istruzioni riducono il rischio di paga-menti irregolari ed errori