LA SICUREZZA DEI PAGAMENTI VIA INTERNET

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

YAP ti offre la massima tranquillità anche in internet, 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, uno smartphone o un Tablet:

- installa e mantieni sempre aggiornato il software di protezione antivirus (i) e antispyware
- installa gli aggiornamenti della App YAP
- 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: YAP 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 YAP: come crearla e proteggerla

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 di 6 caratteri numerici non usando numeri consecutivi crescenti o decrescenti oppure lo stesso numero;
- non utilizzare password condivise con altri servizi online;
- non comunicare la password con amici, conoscenti, operatori del Servizio Clienti YAP. Ti ricordiamo che YAP non ti chiederà mai di comunicare o inviare la tua password né telefonicamente né via mail.

YAP: Tutela i tuoi acquisti in internet

Con la App YAP puoi utilizzare la tua Carta in tutta tranquillità anche per le tue spese online, grazie al servizio 3D Secure che viene abilitato al momento dell'Enrollment.

Al momento del pagamento, ricevi una notifica dall'App al numero di cellulare utilizzato per la tua registrazione a YAP.

Cosa fare in caso di furto/smarrimento dei tuoi dispositivi o delle tue carte o in caso di pagamenti anomali

Se perdi, o ti viene sottratto il tuo dispositivo personale (o la tua Carta se richiesta), 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 Servizio Clienti YAP attivo dalle 09 alle 23, 7 giorni su 7 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 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.

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. 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 tua Carta Prepagata. Sappi che, per politiche di antiphishing, YAP non ti chiederà 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 abbia il lucchetto verde. 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 sen sibili (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.

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. YAP non ti chiederà mai di comunicare o inserire telefonicamente i tuoi codici identificativi.

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

Sia YAP 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 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 YAP nelle modalità indicate in precedenza. Inoltre, se controllando le tue spese, trovi una che ritieni di non aver fatto o sulla quale vuoi maggiori informazioni, il Servizio Clienti avvierà le eventuali verifiche.

RICORDA: hai 60 giorni di tempo per inviarci eventuali contestazioni relative alle operazioni addebitate. Puoi contattare il Servizio Clienti YAP per avviare l'eventuale pratica di contestazione.