



INFORMAZIONI DI SICUREZZA FRODI INFORMATICHE



Gentile Cliente,

il maggiore utilizzo dei canali online ha prodotto un sensibile incremento delle frodi finanziarie.

La protezione dei Tuoi dati personali ci sta a cuore! Fai attenzione quando navighi in rete: non diffondere involontariamente le Tue informazioni riservate e presta attenzione a pochi semplici consigli che di seguito Ti forniremo.

Ti proponiamo, infatti, una breve illustrazione delle principali tecniche messe in atto nei confronti dei clienti e alcuni semplici suggerimenti per tutelare i Tuoi dati personali.

Ti ricordiamo che spesso, il punto di partenza delle frodi online si annida in attività apparentemente ordinarie; il pericolo, infatti, potrebbe celarsi dietro l'apertura di un banale allegato oppure un semplice clic a un link.

Potresti essere contattato per fini illeciti tramite e-mail (phishing), SMS (smishing), WhatsApp o telefonate (vishing) con l'obiettivo di ottenere Tue informazioni riservate come dati bancari, numeri di carte di credito, pin del Tuo telefono, password per accedere alle e-mail e codici del Tuo internet banking.

In alcuni casi, per agganciare le vittime, i malviventi sfruttano le modalità appena descritte anche in modo combinato. È plausibile inoltre che, al fine di raccogliere informazioni confidenziali, come abitudini e preferenze di acquisto, potrebbero avere monitorato le Tue abitudini mediante l'utilizzo dei social network.

Non farTi prendere dal panico, impara a difenderTi dalle minacce a cui esponi i Tuoi dati personali seguendo queste semplici regole:

1. Usa sempre il buonsenso, quando vieni contattato con qualsiasi mezzo da un soggetto sconosciuto, controlla sempre la provenienza delle comunicazioni e verifica l'attendibilità del mittente confrontando i dati ufficiali reperibili sul sito web www.bplajatico.it;

2. Non fornire mai i Tuoi dati personali: se Ti vengono richiesti via e-mail, SMS, WhatsApp o per telefono password, numeri di carta di credito, pin o password del Tuo conto online o qualsiasi altra credenziale di sicurezza, rifiuta di procedere ed interrompi ogni forma di conversazione;
3. Se vieni contattato da un mittente sconosciuto via e-mail, SMS o WhatsApp, non cliccare sul link e non scaricare l'allegato e le immagini che contengono;
4. Se vieni contattato via e-mail, SMS o WhatsApp da un mittente che si qualifica come dipendente della Banca Popolare di Lajatico, ricordaTi di verificare l'identità del Tuo interlocutore contattando preventivamente la Tua Filiale di fiducia;
5. Elimina sempre i messaggi e-mail, SMS, WhatsApp sospetti contenenti dei link;
6. Fai attenzione ai dettagli e controlla bene il testo che Ti viene inviato, spesso le false comunicazioni presentano errori grammaticali;
7. Se scarichi i messaggi di posta sul computer, assicurati che la cartella di posta indesiderata sia attiva;
8. Se vieni contattato via e-mail, verifica l'indirizzo di posta elettronica rispondendo al messaggio per verificare se l'indirizzo del destinatario risulta inesistente, in caso di esito positivo, cancella ogni forma di comunicazione;
9. Scarica applicazioni solo da App Store o da Google Play, mai direttamente da un messaggio WhatsApp o SMS;

Ti ricordiamo che nessuno, nemmeno gli addetti della Banca Popolare di Lajatico, sono autorizzati a conoscere e richiedere i Tuoi dati di sicurezza, in quanto riservati; Ti invitiamo dunque a custodire con cura gli stessi e a non diffonderli per nessuna ragione.

Per maggiori informazioni puoi visitare la "Sezione sicurezza" disponibile sul sito www.inbank.it o consultare la medesima informativa accedendo direttamente dal sito internet www.bplajatico.it.

Ti ricordiamo, infine, che la Tua filiale di fiducia resta a completa disposizione per ogni dubbio o necessità.