CASSA DI RISPARMIO
DI FOSSANO SPA

COMUNICAZIONE URGENTE:
segnalazione invio mail sospette
con richiesta di dati ed informazioni personali

Sono stati segnalati alcuni casi di e-mail sospette inviate a clienti della Cassa di Risparmio di Fossano SpA aderenti al servizio CRF Online.

Ricordiamo che la Cassa di Risparmio di Fossano **NON RICHIEDE in alcun caso**, **direttamente o tramite terzi, dati, informazioni personali o codici di accesso al servizio. Allo stesso modo non sono valide presunte promesse di rimborsi economici per chi confermerà i propri codici d'accesso ai servizi internet, all'interno di specifici box.**

Se dovessi ricevere una comunicazione (via email o altro) con la richiesta di dati personali anche se APPARENTEMENTE proveniente dalla Cassa di Risparmio di Fossano, Ti raccomandiamo di **NON rispondere**.

Nel caso avessi già erroneamente inserito i tuoi dati personali, ti invitiamo a:

A. provvedere immediatamente a **modificare il PIN di accesso al servizio,** utilizzando l'apposita sezione del CRF Online (icona con la chiave nel menù superiore);
B. **contattare** subito il Servizio Assistenza Clienti al **n. 848 800.156 per i telefoni fissi e al n. 02 3340.8972 per i cellulari**

Sottolineiamo che per le operazioni di importo elevato, il CRF Online garantisce ulteriormente la Tua sicurezza con l'utilizzo bloccante di password usa & getta contenute nella tessera Password card spedita via posta ordinaria al momento dell'attivazione del servizio.
In ogni caso, in caso di inattività superiore ai 15 minuti il sistema prudenzialmente disattiva la sessione di lavoro.

Di seguito riportiamo le alcune raccomandazioni da seguire per incrementare la propria sicurezza informatica.

1. **La Cassa di Risparmio di Fossano NON richiede codici, password, PIN, numeri di carte di pagamento o altre informazioni riservate tramite posta elettronica. E' pertanto necessario diffidare di e-mail, anche se ricevute da mittenti conosciuti, dove vengono richiesti dati riservati**.

2. **E' consigliabile verificare preventivamente il mittente dei messaggi di posta elettronica;** sono generalmente indici di sospetto la presenza di:
   - indirizzo del mittente in formato web (es.: nome.cognome@dominio);
   - messaggi non personalizzati / generiche richieste di informazioni personali o riservate, per motivi non ben specificati (es.: scadenza dei codici, smarrimento, problemi tecnici o di sicurezza, ecc.);
   - toni "intimidatori" (es. minacce di sospensione del servizio in caso di mancata risposta) che non sono mai presenti in comunicazioni della nostra Banca.

3. **Al ricevimento di e-mail SOSPETTE**, è sempre necessario **EVITARE di attivare i link** presenti nei messaggi (con un clic del mouse sullo stesso link), e/o **EVITARE di aprire file eventualmente allegati**. In particolare i siti web proposti, soprattutto se richiedono informazioni riservate o password, non vanno visitati neppure per brevi periodi, in quanto:
   - il link proposto potrebbe non essere quello "visualizzato" ed i file ricevuti potrebbero comportare rischi;
   - questi collegamenti potrebbero condurre ad un sito maligno opportunamente contraffatto, difficilmente distinguibile dall'originale.

   Anche se sulla barra degli indirizzi del browser viene visualizzato l'indirizzo corretto, non vi fidate: l'indirizzo Web visualizzato potrebbe essere stato alterato dal truffatore. **La Cassa di Risparmio di Fossano richiede ai propri Clienti di inserire i dati di autenticazione personale o altre informazioni riservate SOLO nel proprio sito https://online.crfossano.it.**

4. **Durante la navigazione nella rete Internet, è necessario evitare di fornire informazioni finanziarie ovvero dati riservati** in qualsiasi sito Web, senza aver preventivamente verificato che:
   - il protocollo di trasmissione risulti "sicuro" (protocollo di sicurezza SSL*), con:
     → presenza del suffisso **HTTPS://** nell'indirizzo web;
     → evidenza dell'icona a forma di "lucchetto chiuso" di colore oro nella barra di stato del browser
   - il sito Web risulti autentico tramite la verifica del **certificato Verisign** (doppio clic sull'icona a forma di lucchetto chiuso.

   * Il suddetto protocollo sicuro, adottato dalla Cassa di Risparmio di Fossano SpA, ha lo scopo di proteggere e di garantire la riservatezza delle informazioni del Cliente durante l'utilizzo dei nostri servizi bancari via Internet.

5. **E' opportuno evitare il "salvataggio automatico" delle credenziali di autenticazione o delle password nelle memorie locali del browser e/o del Personal Computer utilizzato per la navigazione**; in particolare è preferibile verificare che la funzione di "completamento automatico" del browser non risulti attiva. Si ricordano i passaggi per disattivarla,
   - utilizzando **INTERNET EXPLORER:**
     → clic sul menu' Strumenti – Opzioni Internet – Contenuto – Completamento automatico;
     → se presente, eliminazione segno spunta dalle voci "Nome utente e password sui moduli" e "Richiedi salvataggio password";
     → clic sui pulsanti "Cancella moduli" e "Cancella password" (in questo modo verranno cancellate TUTTE le password memorizzate);
     → clic su OK.

- utilizzando **NETSCAPE:**
  → clic sul menu' Edit – Preferences - Privacy & Security" - "Password";
  → se presente, eliminazione del "flag" da "Remember Password";
  → clic su OK.

6. **E' opportuno adottare prodotti software che prevedano filtri per la posta indesiderata.** Questi sistemi, come le più recenti edizioni dei programmi utilizzati per la gestione della posta elettronica, sono in grado di attenuare i rischi filtrando molte email inviate con scopi illeciti, ovvero pericolose.

7. **E' consigliato utilizzare e mantenere aggiornato un idoneo Software Antivirus.** Le email inoltrate per scopi fraudolenti possono contenere anche programmi maligni, creati allo scopo di carpire e di trasmettere dati personali riservati all'elaboratore utilizzato dal criminale. I prodotti Antivirus più aggiornati sono in grado di intercettare la maggior parte di tali pericolosi programmi.

8. **E' opportuno utilizzare e mantenere aggiornato un Personal Firewall.** L'impiego di questo programma di sicurezza, soprattutto durante la navigazione in Internet, previene lo scambio di comunicazioni indesiderate in ingresso o in uscita dal Personal Computer utilizzato dall'Utente e risulta indispensabile in caso di eventuale utilizzo di programmi di condivisione di file su Internet.

9. **E' opportuno aggiornare periodicamente il Sistema Operativo e tutti i programmi utilizzati**. Le aziende produttrici dei Sistemi Operativi, dei browser, ecc. rendono periodicamente disponibili online, gli aggiornamenti agli stessi (le cosiddette patch), che incrementano la sicurezza di questi programmi, prevenendo l'utilizzo fraudolento delle cosiddette "vulnerabilità" che potrebbero essere sfruttate dai criminali informatici.

10. **E' opportuno segnalare all'Autorità Giudiziaria o di Polizia ed alla Banca il ricevimento di e-mail aventi scopi o contenuti fraudolenti**, evitando di rispondere a tale messaggio. La denuncia alle Autorità, in casi costituenti reato, consente alle stesse un immediato intervento ed alla Banca colpita di attivare contromisure difensive a tutela dei propri Clienti.

11. **E' consigliabile diffidare di improvvisi cambiamenti di modalità con la quale viene chiesto di inserire i vostri codici di accesso all'home banking (soprattutto se non comunicati in via ufficiale).** Un caso comune è dato dalla richiesta di inserimento dei dati tramite inusuali finestre di pop-up (una finestra aggiuntiva di dimensioni ridotte), in caso di dubbio è bene contattare la propria Filiale o telefonare al Servizio di Assistenza Clienti.

12. E' comunque oppurtuno:
    - **esaminare periodicamente la propria movimentazione;**
    - **modificare periodicamente il codice PIN;**
    - **NON utilizzare i codici per il CRF Online anche per altri servizi.**