SPARKASSE
CASSA DI RISPARMIO

REGOLE PER NON CADERE IN TRUFFE TIPO PHISHING

1. Diffidate di qualunque **mail che vi richieda l'inserimento di dati** riservati riguardanti codici di carte di pagamento, password e PIN di accesso al servizio internet banking o altre informazioni personali. Noi non richiederemo mai tali informazioni via e-mail.

2. È possibile riconoscere **le truffe via e-mail** con qualche piccola attenzione. Generalmente queste e-mail:
   - non sono personalizzate e contengono un messaggio generico di richiesta di informazioni personali per motivi non ben specificati (es. scadenza, smarrimento, problemi tecnici)
   - fanno uso di toni "intimidatori", ad esempio minacciando la sospensione dell'account in caso di mancata risposta da parte dell'utente
   - non riportano una data di scadenza per l'invio delle informazioni

3. Nel caso in cui riceviate un'e-mail contenente richieste di questo tipo, **non rispondete all'e-mail stessa**, ma informate subito la vostra banca, la Cassa di Risparmio di Bolzano, tramite Help-Desk o recandovi in filiale.

4. **Non cliccate su link presenti in e-mail sospette**, in quanto questi collegamenti potrebbero condurvi a un sito contraffatto, difficilmente distinguibile dall'originale. Anche se sulla barra degli indirizzi del browser viene visualizzato l'indirizzo corretto, non vi fidate: è possibile infatti per un hacker visualizzare nella barra degli indirizzi del vostro browser un indirizzo diverso da quello nel quale realmente vi trovate.
   Buona norma è digitare espressamente l'indirizzo della pagina web del sito della vostra banca: "www.caribz.it" o www.sparkasse.it.

5. Diffidate inoltre di **e-mail con indirizzi web molto lunghi**, contenenti caratteri inusuali.

6. Quando inserite dati riservati in una pagina web, assicuratevi che si tratti di una pagina protetta: queste pagine sono riconoscibili in quanto l'indirizzo che compare nella barra degli indirizzi del browser comincia con **"https:**//" e non con "http://" e nella pagina (in posizione diversa seconda il tipo e versione del browser utilizzato) è presente un lucchetto; quale ulteriore buona norma, prestate attenzione affinchè la visualizzazione della pagina web della banca avvenga nell'unica finestra aperta del browser.

7. Diffidate se improvvisamente **cambia la modalità** con la quale vi viene chiesto di inserire i vostri codici di accesso all'internet banking: ad esempio, se questi vengono chiesti non tramite una pagina del sito, ma tramite pop-up (una finestra aggiuntiva di dimensioni ridotte). In questo caso, contattate la vostra banca, la Cassa di Risparmio di Bolzano, tramite Help-Desk o recandovi in filiale.

8. **Controllate regolarmente gli estratti conto** del vostro conto corrente e delle carte di credito per assicurarvi che le transazioni riportate siano quelle realmente effettuate. In caso contrario, contattate la vostra banca, la Cassa di Risparmio di Bolzano e/o l'emittente della carta di credito.

9. Le aziende produttrici dei browser rendono periodicamente disponibili on-line e scaricabili gratuitamente degli **aggiornamenti** (cosiddette patch) che incrementano la sicurezza di

questi programmi. Sui siti di queste aziende è anche possibile verificare che il vostro browser sia aggiornato; in caso contrario, è consigliabile scaricare e installare le patch.

10. Internet è un po' come il mondo reale: come non dareste a uno sconosciuto il codice PIN del vostro bancomat, allo stesso modo occorre essere estremamente **diffidenti nel consegnare i vostri dati riservati** senza essere sicuri dell'identità di chi li sta chiedendo. In caso di dubbio, rivolgetevi alla vostra banca, la Cassa di Risparmio di Bolzano!

Per informazioni potete rivolgerVi al Help Desk
Numero telefonico 840.052.052
Indirizzo e-mail: info@sparkasse.it

Si ricorda inoltre che competenze istituzionali in materia di contrasto ai reati informatici spettano alla Polizia Postale.