Proteggiti dalle frodi on line

La protezione dei tuoi dati è la nostra priorità.
Reale Group offre avanzati livelli di sicurezza nell'utilizzo dei sistemi online ma è fondamentale che anche tu sappia come proteggerti da chi finge di essere Il tuo partner assicurativo.
Il crescente utilizzo dei servizi digitali ha infatti reso sempre più frequenti i tentativi di frode informatica.
Vediamo più nel dettaglio queste le diverse tipologie di truffe online in cui i frodatori si spacciano per il tuo Partner Assicurativo.
Queste tecniche, basate sull'inganno e sulla manipolazione psicologica, mirano a sottrarre dati personali, bancari o assicurativi sfruttando canali apparentemente sicuri come e-mail e SMS.
Riconoscere tempestivamente i segnali di un attacco e adottare le giuste misure di protezione è essenziale per tutelare la propria identità digitale e prevenire danni economici.

Scopri come riconoscerle e proteggerti

Phishing

Il phishing è una truffa effettuata tramite e-mail. Il termine deriva dall'inglese "fishing" (pescare) e indica tentativi di frode via posta elettronica.

Smishing

Lo smishing è una variante del phishing che utilizza gli SMS.
I truffatori inviano messaggi di testo fingendosi il tuo Partner Assicurativo per acquisire informazioni personali, finanziarie o di sicurezza.

Vishing

Il vishing, abbreviazione di "voice phishing", è una frode telefonica in cui i truffatori tramite una chiamata telefonica cercano di indurre la vittima a divulgare informazioni personali, finanziarie o di sicurezza o a trasferire loro del denaro.

Come Riconoscere Phishing, Smishing e Vishing

In tutte queste forme di frode, la comunicazione sembra provenire da una fonte attendibile, come il tuo Partner assicurativo, banche, società di carte di credito o siti web che richiedono registrazione.

Solitamente, i messaggi sono progettati per indurre l'utente a rivelare dati riservati, facendo leva su falsi problemi di registrazione o di altro genere.

Segnali di Allarme

1. **Link sospetti**: Il messaggio include un link che sembra condurre al sito dell'istituto di credito ma in realtà porta a un sito clone.
2. **Richieste urgenti**: Sollecitazioni a fornire informazioni personali o a risolvere problemi urgenti.

3. **Errori grammaticali**: Errori di ortografia o grammatica nel messaggio.

Come Proteggersi

• **Verifica la fonte**: Non cliccare su link o fornire informazioni tramite e-mail, SMS o telefonate non richieste.
• **Controlla l'URL**: Assicurati che l'indirizzo web sia corretto e non contenga variazioni sospette.
• **Usa l'autenticazione a due fattori**: Aggiungi un ulteriore livello di sicurezza ai tuoi account.

Se pensi di essere stato vittima di un tentativo di frode online, avvisa subito la Compagnia. Denuncia, inoltre, l'accaduto all'Autorità Giudiziaria o di Polizia.
Le segnalazioni possono attivare contromisure immediate per proteggere gli altri Clienti.
Reale Group non ti richiederà mai di comunicare per via telefonica, SMS o e-mail password dispositive e/o di accesso (codice utente, password, OTP).
Controlla ogni particolare di tutte le comunicazioni che ti vengono inviate, tutela la riservatezza dei tuoi dati personali e diffida da qualsiasi contatto telefonico che richieda tali informazioni.
I dettagli fanno la differenza per prevenire al meglio il rischio di frode.
In caso di dubbio è consigliabile chiamare il servizio clienti al numero ufficiale, consultare i portali antifrode di IVASS o le segnalazioni della Polizia Postale.