AVVISO IMPORTANTE: TENTATIVI DI FRODE TRAMITE FURTO D'IDENTITA

Come molte altre aziende, stiamo assistendo a un aumento dei tentativi di frode che utilizzano in modo improprio il nome, l'identità visiva o i recapiti della nostra azienda, in particolare attraverso la creazione di nomi di dominio falsi volti a ingannare la vigilanza dell'interlocutore e, in alcuni casi, quella di ex collaboratori su applicazioni di messaggistica istantanea.

Queste azioni hanno lo scopo di indurre in errore gli investitori proponendo loro prodotti finanziari falsi, false opportunità di investimento o tentando di ottenere informazioni personali o bancarie.

Vi raccomandiamo di prestare attenzione per proteggervi e vi ricordiamo che:

- Il nostro sito web ufficiale è https://www.comgest.com.
- Comgest non utilizza i social network e le applicazioni di messaggistica istantanea (come WhatsApp) come mezzo di contatto.

➢ Frode e furto d'identità

La frode è un atto intenzionale di inganno o occultamento volto a ottenere un vantaggio indebito a danno di altri. Comprende un'ampia gamma di comportamenti sleali, come l'usurpazione di identità quando viene utilizzata per scopi dolosi.

L'usurpazione di identità consiste nell'appropriarsi consapevolmente dell'identità di una persona fisica o giuridica, o nell'utilizzare i suoi elementi identificativi (nome, logo, indirizzo e-mail, documenti ufficiali) allo scopo di ingannare terzi. Quando mira a ottenere un vantaggio indebito o a causare un danno, l'usurpazione di identità costituisce una forma di frode e può anche essere considerata una truffa.

➢ Quali riflessi adottare per proteggersi da una frode?

- Prestare la massima attenzione a qualsiasi contatto non richiesto tramite telefono, e-mail, SMS, social network o applicazioni di messaggistica istantanea. Qualunque sia la forma (telefono, posta, e-mail o messaggio), le usurpazioni sono frequenti, numerose e facili da realizzare.

- Non comunicate alcuna informazione personale (numero di telefono, e-mail, documenti di identità, coordinate bancarie, IBAN, prove di residenza...) tramite un sito web o per telefono a una persona che dichiara di rappresentarci, senza averne verificato l'autenticità attraverso i nostri canali ufficiali.

- Informatevi sulla società di cui il vostro interlocutore dichiara di far parte cercando i suoi recapiti ufficiali (numero di telefono, indirizzo e-mail e postale) tramite altre fonti al fine di verificare la veridicità delle informazioni fornite e non esitate a verificare l'identità dei vostri interlocutori inviando un'e-mail o chiamando i numeri di telefono indicati sui siti ufficiali.

- Se un messaggio vi sembra provenire da una fonte sconosciuta o dubbia, fate attenzione a non cliccare sui link né ad aprire gli allegati e non rispondete.

Per ulteriori raccomandazioni, vi invitiamo a consultare le informazioni didattiche pubblicate online dall'Autorità dei Mercati Finanziari in Francia o dal vostro regolatore locale.

➢ Cosa fare se pensate di essere stati vittime di una frode?

1. Se la frode è correlata a Comgest, informateci direttamente all'indirizzoinfo@comgest.com .

2. In caso di furto d'identità tramite WhatsApp, segnalate il messaggio, il gruppo e/o il profilo sospetto come segue, quindi eliminate il messaggio dal vostro dispositivo dopo averlo segnalato:
   - Segnalazione di un profilo: cliccate sul contatto da segnalare, quindi, in fondo alla pagina, cliccate su "Segnala + numero di telefono".
   - Segnalazione di un gruppo: clicca sul nome del gruppo nella parte superiore delle chat, quindi, in fondo alla pagina, clicca su "Segnala il gruppo".

3. Se sei cittadino francese, effettua una segnalazione Pharos (portale ufficiale del Ministero dell'Interno per la segnalazione di contenuti illegali su Internet): https://internet-signalement.gouv.fr/.