

Wie viele Unternehmen beobachten auch wir eine **Zunahme von Betrugsversuchen**, bei denen der **Name, das visuelle Erscheinungsbild oder die Kontaktdaten unseres Unternehmens missbräuchlich verwendet werden** – insbesondere durch die Erstellung gefälschter Domainnamen, die darauf abzielen, Empfänger zu täuschen, und in manchen Fällen auch durch die **Verwendung der Identität ehemaliger Mitarbeitender in Instant-Messaging-Anwendungen**.

Diese Vorgehensweisen haben zum Ziel, Investoren in die Irre zu führen, indem ihnen gefälschte Finanzprodukte, falsche Anlagegelegenheiten angeboten werden oder indem versucht wird, persönliche oder Bankdaten zu erlangen.

Wir empfehlen Ihnen, wachsam zu sein, um sich zu schützen, und erinnern daran, dass:

- **Unsere offizielle Website lautet: <https://www.comgest.com>.**
- **Soziale Netzwerke und Instant-Messaging-Anwendungen (wie WhatsApp) werden von Comgest nicht als Kontaktmittel verwendet.**

#### ➤ **Betrug und Identitätsdiebstahl**

**Betrug** bezeichnet eine vorsätzliche Täuschung oder Verschleierung mit dem Ziel, sich auf Kosten anderer einen unrechtmäßigen Vorteil zu verschaffen. Er umfasst eine Vielzahl unlauterer Handlungen, wie etwa den Identitätsdiebstahl, wenn dieser zu böswilligen Zwecken eingesetzt wird.

**Identitätsdiebstahl** bedeutet, sich wissentlich die Identität einer natürlichen oder juristischen Person anzueignen oder deren Identifikationsmerkmale (Name, Logo, E-Mail-Adresse, offizielle Dokumente) zu verwenden, um einen Dritten zu täuschen. Wenn er darauf abzielt, einen unrechtmäßigen Vorteil zu erlangen oder einen Schaden zu verursachen, stellt Identitätsdiebstahl eine Form von Betrug dar und kann zudem den Tatbestand des Betrugs/der Täuschung erfüllen.

#### ➤ **Welche Maßnahmen sollten Sie ergreifen, um sich vor Betrug zu schützen?**

- Begegnen Sie jeder unaufgeforderten Kontaktaufnahme per Telefon, E-Mail, SMS, über soziale Netzwerke oder Instant-Messaging-Anwendungen mit größter Vorsicht. Unabhängig von der Form (Telefon, Brief, E-Mail oder Nachricht) sind Identitätsanmaßungen häufig, zahlreich und leicht umzusetzen.
- Geben Sie keine persönlichen Informationen (Telefonnummer, E-Mail, Ausweisdokumente, Bankverbindung, IBAN, Wohnsitznachweise usw.) über eine Website oder telefonisch an Personen weiter, die behaupten, uns zu vertreten, ohne deren Echtheit über unsere offiziellen Kanäle überprüft zu haben.
- Informieren Sie sich über das Unternehmen, auf das sich Ihr Ansprechpartner beruft, indem Sie dessen offizielle Kontaktdaten (Telefon, E-Mail- und Postadresse) über andere Quellen recherchieren, um die Richtigkeit der Angaben zu prüfen. Zögern Sie nicht, die Identität Ihrer Ansprechpartner zu verifizieren, indem Sie eine E-Mail senden oder die auf den offiziellen Websites angegebenen Telefonnummern anrufen.

- Wenn Ihnen eine Nachricht aus unbekannter oder zweifelhafter Quelle zu stammen scheint, klicken Sie nicht auf Links, öffnen Sie keine Anhänge und antworten Sie nicht darauf.

➤ **Was tun, wenn Sie glauben, Opfer eines Betrugs geworden zu sein?**

1. Wenn dieser **Betrug mit Comgest in Zusammenhang** steht, informieren Sie uns direkt unter: [info@comgest.com](mailto:info@comgest.com)
2. Im Falle einer **Identitätsanmaßung über WhatsApp** melden Sie die Nachricht, die **Gruppe und/oder das verdächtige Profil** wie folgt und löschen Sie die Nachricht nach der Meldung von Ihrem Gerät:
  - **Meldung eines Profils:** Tippen Sie auf den zu meldenden Kontakt und klicken Sie unten auf der Seite auf „Melden + Telefonnummer“.
  - **Meldung einer Gruppe:** Tippen Sie oben in den Chats auf den Gruppennamen und klicken Sie unten auf der Seite auf „Gruppe melden“.
3. Wenn Sie sich in Deutschland aufhalten bzw. Ihren Wohnsitz, können Sie über die **Onlinewache der Polizei (je Bundesland** Betrug/Cybercrime online anzeigen bzw. melden. <https://portal.onlinewache.polizei.de/de/>
4. Wenn Sie die **französische Staatsangehörigkeit** besitzen, erstatten Sie eine Meldung über Pharos (offizielles Portal des Innenministeriums für Meldungen illegaler Internetinhalte): <https://internet-signalement.gouv.fr/>.