# Guida alla Prevenzione delle Frodi Digitali e AI-Based

Proteggersi oggi per non pentirsene domani

La sicurezza delle tue informazioni e dei tuoi fondi è una priorità per 3Rooks Money S.p.A. Per aiutarti a riconoscere e prevenire i tentativi di frode più diffusi, abbiamo preparato questa guida pratica.

## Frode BEC – Business Email Compromise

Ricevi un'email che sembra provenire da 3Rooks o da un fornitore/partner aziendale, con istruzioni per trasferire fondi su un nuovo conto.

- Controlla sempre l'indirizzo email completo del mittente.
- Non effettuare mai bonifici su conti nuovi senza una conferma tramite messaggistica interna o contatto ufficiale.
- In caso di dubbio, contatta direttamente il servizio clienti 3Rooks.

## Frode di phishing

Ricevi email, SMS o messaggi che imitano comunicazioni ufficiali e ti invitano a cliccare su un link per aggiornare dati, accedere al tuo conto o risolvere problemi urgenti.

- Non cliccare su link sospetti o non richiesti.
- Verifica sempre che il sito web inizi con https e che l'indirizzo sia corretto.
- 3Rooks non chiederà mai credenziali o dati personali via email, SMS o telefono.

## Frodi da impersonificazione su social media o app di messaggistica

Ricevi un messaggio da qualcuno che si finge un parente, amico o funzionario. Chiede denaro, favori, prestiti o accessi al tuo conto.

- Verifica sempre l'identità con una chiamata diretta.
- Non fornire mai codici, credenziali o dati personali tramite app di messaggistica.
- Non aprire conti su richiesta di terzi, anche se sembrano affidabili.

## Frode da piattaforme di trading online

Vieni attirato da annunci o "esperti" che ti promettono guadagni facili tramite investimenti in criptovalute o forex su piattaforme non autorizzate.

- Controlla sempre che la piattaforma sia autorizzata da autorità competenti.
- Diffida da chi ti spinge a investire con urgenza o ti offre bonus garantiti.
- Non effettuare investimenti  tramite canali non ufficiali.

# Frodi basate su Intelligenza Artificiale

L'intelligenza artificiale viene usata sempre più spesso per realizzare truffe sofisticate. Ecco i principali rischi:

## Deepfake

Video, audio o immagini creati per imitare volti e voci reali (es. un finto video del CEO che ti chiede un bonifico urgente).

- Non agire mai sulla base di contenuti multimediali senza verifica diretta con la persona interessata.

## Raccolta illecita di dati (sorveglianza AI)

Algoritmi che raccolgono e analizzano i tuoi dati da fonti pubbliche o violando la tua privacy.

- Proteggi i tuoi profili social, limita la condivisione di dati sensibili e usa software aggiornati.

## Attacchi automatizzati

AI usata per effettuare attacchi di tipo 'brute force', trovare falle nei software o accedere a sistemi vulnerabili.

- Usa password complesse, cambia regolarmente le credenziali e attiva l'autenticazione a due fattori.

## Chatbot malevoli e disinformazione

Chat o assistenti automatici che fingono di essere supporto tecnico o operatori per estorcere dati o denaro.

- Comunica solo con operatori tramite la piattaforma ufficiale di 3Rooks.

## IA usata per frodi finanziarie

Algoritmi intelligenti progettati per simulare il comportamento umano, aggirare controlli e truffare piattaforme.

- Sospetta sempre di offerte troppo vantaggiose, specie se provengono da fonti non verificate.

# Cosa fare in caso di dubbio

In caso di comunicazioni sospette:

- Non rispondere, non cliccare e non inviare denaro o dati.
- Segnala subito l'accaduto tramite la messaggistica interna di 3Rooks Money S.p.A.
- Conserva prove (screenshot, email, messaggi).
- Contatta le autorità competenti