Guide to Preventing Digital and AI-Based Fraud

Protect Yourself Today to Avoid Regrets Tomorrow

At 3Rooks Money S.p.A., the security of your information and funds is a top priority. To help you recognize and prevent the most common types of fraud, we have prepared this practical guide.

BEC Fraud – Business Email Compromise

You receive an email that appears to come from 3Rooks or a business supplier/partner, instructing you to transfer funds to a new account.

- Always check the sender's full email address.
- Never transfer funds to a new account without confirmation via internal messaging or an official contact.
- If in doubt, contact 3Rooks Customer Service directly.

Phishing fraud

You receive emails, SMS messages, or other communications imitating official ones, urging you to click on a link to update information, access your account, or resolve an urgent issue.

- - Do not click on suspicious or unsolicited links.
- - Always verify that the website address begins with https and is correct.
- - 3Rooks will never ask for credentials or personal data via email, SMS, or phone.

Impersonation Fraud via Social Media or Messaging Apps

You receive a message from someone pretending to be a relative, friend, or official, asking for money, favors, loans, or access to your account.

- Always verify the identity with a direct phone call.
- Never share codes, credentials, or personal data through messaging apps.
- Never open accounts at the request of third parties, even if they seem trustworthy.

Online Trading Platform Fraud

You are drawn in by ads or "experts" promising easy profits through investments in cryptocurrencies or forex via unauthorized platforms.

- Always check that the platform is authorized by relevant authorities.
- Be wary of anyone pushing you to invest urgently or offering guaranteed bonuses.
- Do not make investments through unofficial channels.

AI-Based Fraud

Artificial intelligence is increasingly used to carry out sophisticated scams. Here are the main risks:

➢ Deepfake

Videos, audio, or images created to mimic real faces and voices (e.g., a fake video of the CEO requesting an urgent bank transfer).

- Never act based on multimedia content without directly verifying with the actual person.

➢ Illicit Data Collection (AI Surveillance)

Algorithms that collect and analyze your data from public sources or by violating your privacy.

- Protect your social media profiles, limit sharing of sensitive data, and keep your software updated.

➢ Automated Attacks

AI used to perform brute-force attacks, find software vulnerabilities, or access weak systems.

- Use strong passwords, update your credentials regularly, and enable two-factor authentication.

➢ Malicious Chatbots and Disinformation

Chat or virtual assistants pretending to be technical support or agents to extract data or money.

- Only communicate with agents through the official 3Rooks platform.

➢ AI Used in Financial Fraud

Smart algorithms designed to simulate human behavior, bypass controls, and defraud platforms.

- Always be skeptical of offers that seem too good to be true, especially from unverified sources.

What to Do If You're Unsure

In case of suspicious communications:

- Do not respond, click, or send money or data.

- Report the incident immediately via the internal messaging system of 3Rooks Money S.p.A.

- Keep evidence (screenshots, emails, messages).

- Contact the relevant authorities.