CLEOPATRA

Total Project & Turnaround Management Platform

Cleopatra Enterprise

Fraud Awareness policy

At Cleopatra Enterprise, safeguarding your financial security is our priority. We are committed to maintaining transparency and providing you with the necessary information to protect yourself against fraud and phishing attempts. To help you stay protected, this page provides important guidelines on recognizing potential threats, verifying our official communication channels, and knowing what to do if you suspect fraudulent activity.
If you are contacted with a message claiming that we have changed our bank account number, please remain cautious, and follow the instructions outlined below to verify the authenticity of the communication.

How to Protect Yourself Against Fraud and Phishing

Cybercriminals may attempt to impersonate our company or misuse our bank account details to deceive clients. To help you stay protected:

- No unexpected changes
  - We will communicate any changes to our bank account number well in advance of the actual change through our financial department.
  - The only ones in the company who can sign any forms are our CEO and Managing Director. No other employees can fill in and sign change forms for our clients.
  - We will never notify you of bank account changes via email, SMS, or phone calls from unknown phone numbers.
- Before making any payment, verify that the account number matches the details provided by our finance department or contact your Cleopatra Enterprise contact if you have asked for it previously and potentially previous invoices.
- Always verify payment instructions directly with us through our finance department or your known Cleopatra Enterprise contact, especially if they are sent via email or text message.
- Be cautious of impersonation. If someone you (think to) know suddenly sends unusual requests or financial instructions.
- Potential hackers can try to use a different phone number which looks legitimate through caller ID spoofing. Which is why we recommend looking up our phone number yourself whenever you need to call us. Please do not use the phone number provided in an email, text message or any other communication.

- Potential hackers can try to use a different phone number which looks legitimate through caller ID spoofing. Which is why we recommend looking up our phone number yourself whenever you need to call us. Please do not use the phone number provided in an email, text message or any other communication.

- Check sender email addresses, URLs, and any links before clicking on them.

- Please check if you recognize the sender, if the email address or person signing the email is not familiar, please contact us to verify if this person actually works for Cleopatra Enterprise.

- Email signatures can be verified through previous emails. If there is data missing from the email signature, it might be because the email is fraudulent.

What to Do if You Suspect Fraud

If you receive suspicious communication claiming to be from Cleopatra Enterprise or Cost Engineering B.V., or notice unusual activity related to payments or invoices, please follow these steps:

Do Not Respond:
Avoid interacting with the message, clicking on links, or downloading attachments.

Verify the Source

1. Can always be requested through our finance department or your trusted/known contact at Cleopatra Enterprise
2. If you have any doubts about a received message, please contact our finance department, your contact at Cleopatra Enterprise or call our HQ. +31 (0)78 620 0910
3. We only confirm bank account changes through our financial department.

Report the Incident:
Please forward any suspicious emails or messages to the finance department, or call our HQ +31 (0)78 620 0910.

Stay Informed:
Check our website regularly for updates and tips on how to recognize fraudulent activities.

Resources and Support

For more information on secure payments and fraud prevention or any other topics, please contact our finance department or your trusted Cleopatra Enterprise contact for assistance. Your vigilance helps protect both you and our business from potential security threats. Thank you for partnering with us to ensure a safe and secure transaction process.