SCAM Notice:

Typical Scams

Recruitment Scam: offer of employments falsely on behalf of ISCO. Candidates are contacted by someone claiming to be a representative from ISCO or ISCO's agent. Candidates are interviewed over the phone or via skype and may be referred to ISCO's website for further information. Fake employment offers are sent with ISCO logo and solicit the transfer of money for work permit, visa administration, agency fees, deposit on accommodation, medical check-up, etc. Further, the fraudsters may also ask for personal information such as bank account details to set up salary payments. In reality, any fees paid go to the fraudsters and they stop responding to any communications from the candidates once the fees are wired / transferred.

Advance fee scam: may take many forms but in essence it involves people being persuaded to advance sums of money in the hope of receiving a larger gain. The gain is, however, never realized. The fraudster claims that the target will be reimbursed the upfront fee in the future and once the fee is paid. For example, the targets may receive a business proposal or transaction using the name of ISCO, promise to send products/services, offer to participate in a special deal, solicit contract bids on fictitious projects etc.

Grants/awards Scam: involves unexpected email, letter or call advising that an award/grant has been won. The fraudster will invariably request a fee that is required to improve chances of winning, process the winning, bank fees, government taxes, shipping charges, etc. The fraudster may also request for personal information to confirm the identity of the target and to collect the winning. All claimed winnings are stalled and the fraudsters try to collect as much money in fees and charges.

How to Detect Scams

- ISCO officials do not communicate via generic email addresses such as Hotmail, Yahoo. All communications will always originate from a verifiable ISCO e-mail address (domains of @isco.com.kw) and not from any free web based email accounts.
- Individuals who are successful in gaining an offer of employment from ISCO, whether directly or indirectly are always required to go through a formal recruitment process. During our recruitment

process, the candidate will, in general, meet in person with an ISCO employee or representative for an interview before any formal offer is made.

- Fraudsters usually ask targets to respond quickly or risk missing out.
- Fraudsters usually request targets to keep business proposals, winning, etc confidential.
- Fraudsters usually communicate only via email and telephone with reluctance or a refusal to meet in person.
- Conduct general searches (Google or ISCO Official website) to verify the details provided in false letters and communications (i.e. CEO's name, companies under SEMHA Group).

How to Contact us

You should consider reporting the incident to your local law enforcement.

You may contact ISCO about any suspected scams perpetrated using the name of ISCO through ISCO website:

• ISCO Website: <u>www.isco.com.kw</u>

DISCLAIMER: ISCO shall not be responsible for the content of any information nor shall it be liable for any conclusion, loss or damage of any nature whatsoever suffered or may be suffered by any part or members of the public arising from or as a result of reliance on or usage of any information from portals, websites or e-mail domains which are not authorized by ISCO.