THE AIR LEAGUE

**Social Engineering Fraud**

'Social engineering fraud' is a broad term that refers to the scams used by criminals to trick, deceive and manipulate their victims into giving out confidential information and potentially leading to the loss of funds .

Criminals exploit a person's trust in order to find out their bank details, passwords or other personal data. Scams are carried out online, for example, by email or through social networking sites – telephone, or even in person.

**Who is Targeted?**

Everyone is vulnerable to being targeted, whether as an individual, in their individual capacity in the workplace or the company as an entity.

People of all ages and backgrounds, but especially vulnerable persons, are susceptible to targeting. Our organisation works with persons in these categories and must take all appropriate measures to ensure data is protected and no-one can be made open to being targeted via their association with our organisation.

Everyone within the Air League is expected to adhere to rules and guidelines implemented to maintain these protections.

**How Are People Tricked?**

Social engineering techniques have become extremely sophisticated, messages are designed to appear professional and can be convincing. This is an industry and criminals know how to manipulate people convincingly.

Criminals exploit peoples' trust or their willingness to be help others. This can be especially deleterious in a charity organisation where the ethos is to be of service and assistance to other people. Criminals may also try intimidation tactics to achieve their results. Eg, pretending to be angry customer, threatening the organisation's reputation.

**Protection: Myself, Myself in the Workplace, My Organisation**

**How can I protect myself?**

**Individuals**

Remain vigilant and take the time to assess any e-mails you had not expected to receive. Be sure to check carefully the sender's email address and any URLS and check the authenticity of the information against an official source.

If you receive a message you were not expecting, (even if it appears to be from someone you know), or you get an offer that seems too good to be true:

- Do not open any attachments
- Do not click on any links
- Do not reply
- Do not send any money
- Do not send identification documents – not even copies
- Do not give details of your bank accounts or payment cards
- Report the message as spam through your internet supplier then delete it. Presently, as a small organisation, it is permitted to contact our IT support company directly. Please however CC in your co-workers as:
    - 1) a warning system for them to beware
    - 2) until such time the organisation grows and there is a single point of contact appointee.
    - 3) The organisation expects its Trustees and other organisation designated members (eg Leading Edge) to direct these issues to the office.

Likewise, if you receive a phone call you do not feel comfortable with, do not give any information and end the conversation. As an experienced staff member, your experience may 'tell' you the situation is not quite right.

At any time, if you, as a staff member, Trustee or other stakeholder, have any qualms about any contact or approach that has been made to you, please share this information with the operations team in the office. They are best placed to assist in supporting you and protecting you and your organisational identity.

We also request, that staff and stakeholders protect their PCs and other devices by setting spam filters to the highest level, and installing firewalls and anti-virus software – and keeping them up to date. If assistance is required, please contact the office.

**Companies**

In addition to the steps described above, by protecting yourself, and applying the above to your job role, you can protect the organisation too.

As a complementary measure, we will also make best practice endeavours for the following:

- Rules and guidelines will be put in place for the handling of sensitive information within your company
- Provide training to staff (and stakeholders where applicable) on how to recognise different types of fraud
- Instruct staff to test and verify changes sent via email or other media relating to changes in the supplier information
- Use company procedures to identify suppliers
- Follow company procedures with regard to information requests from unknown parties. Or if new information is provided, confirm this.

- If refund requests are requested, implement re-checking procedures to ensure the right person receives the funds, eg, Card payments; only refund via the original Paypal link, or refund the original card used to make a purchase.
- Use intrusion test to identify vulnerabilities and strengthen security
- A best practice will be used to remain up to date with guidelines and from law enforcement and other appropriate agencies to remain current on the latest trends in social engineering
- Systems put in place require dual authorisations for payments from banks
- Establish contact with bank for key personnel and make best endeavours in requiring them to become familiar with our processes and thus detect any suspicious requests
- Staff become engaged and encouraged to 'Know Your Stakeholder'. It is these incremental steps that will assist in ensuring the continued protection of the Organisation

Due to continual developments in this area, the above list is not exhaustive, and continued engagement and input from all parties is actively encouraged.