BEST PRACTICES TO PREVENT BECOMING A VICTIM OF SOCIAL ENGINEERING FRAUD

Overview

Communication is Key

Increase staff awareness about social engineering fraud at all levels and across all parts of the business, in particular those who are likely to liaise with third parties and clients, not just the finance department. Quite often it's the staff who deal with clients and suppliers every day who will request finance to make ad-hoc payments. Effectively communicating the risk of a social engineering loss only adds an extra defence barrier to preventing a fraud.
Here are some examples and best practices on how to mitigate and stop a social engineering loss occurring.

3 key actions to prevent being a victim:

- ✓ Identify
- ✓ Verify
- ✓ Authenticate

Fake President/CEO Fraud:

- Always speak to the individual who has purportedly sent or given the instruction to make a payment.
- Always verify requests with another director, manager or supervisor and check the bank account is on an approved list which has been vetted.

Telephone Payments & Fund Transfers:

- Avoid giving or accepting payment instructions via telephone or email.
- Only accept requests in writing and on company headed paper from a known point of contact in that organisation.
- Verify all requests with a call back procedure to confirm authenticity.

Suite 3, 110-116 East Parade, East Perth WA 6004
Phone: (08) 6184 8000

Email Scams & Requests to Change Bank Account Details:

- Check the name and email address of sender for spelling mistakes and if they are on approved list of contacts.
- Do not open any emails from unknown senders or with suspicious titles - they could contain viruses and expose the organisation to a cyber attack.
- Where an email appears to be from a known person, click on the email address to ensure it's not hiding a bogus address.
- Using a call back procedure to authenticate the request can avoid being victim to a fraudster impersonating a known contact.
- Check the client file for any history of previous requests to amend bank account details or send large sums to a new account.

Managing Suppliers & Vendor Details:

- Maintain an approved list of suppliers and vendors, including key contacts with email addresses and telephone numbers.
- Ensure Suppliers and Vendors know that any requests to change bank account details should be sent in writing on company headed paper, signed by an approved person.
- Have a dual control procedure in place when appointing new suppliers to prevent fictitious vendor fraud.

Suite 3, 110-116 East Parade, East Perth WA 6004
Phone: (08) 6184 8000