Abbey Tax

Social engineering

Key tips to help avoid cyber crime

One of the fastest-growing cyber crime threats today does not exploit IT or information security weaknesses, rather fraudsters are targeting individuals using deception and impersonation, in order to persude them to give away data. There are steps companies should take to minimise the risk of social engineering attacks and protect IT and data assets. Markel policyholders can also call the cyber risks helpline if they are concerned or need advice on social engineering attacks.

Incoming emails or phone calls

Irrespective of the email or caller ID all requests to alter bank, payment or supply details should be independently verified prior to actioning with a known client contact.

- Introduce additional checks for urgent or unusual transactions
- Raise awareness with all staff of dangers of emails and phone calls being hacked for deception/ impersonation
- Never disclose password or security credentials to any person who has contacted you
- Check default IT settings for any potential improvements in actively filtering suspicious email activity

Implement a written policy for authenticating payment instructions

Procedures: The duties of each employee should be arranged so that no single individual can do all the following:

- Authorise payments above £2,500
- Control any transaction from start to finish
- Issue fund transfer instructions
- Open new accounts or amend fund transfer procedures
- Make investments in shares, other security or valuables

References: Always get written or verbal references to cover a minimum period of two years immediately preceding their employment.

Payments: Ensure that payments for goods and services are authorised by an employee/volunteer who is not responsible for ordering or certifying receipt of such goods or services.

Recovery

If an incident occurs, you should be ready with contact details and personnel to act quickly before these sums are successfully moved out of reach. There may also be contractual recourse against the bank or payment processor. You should also contact **Action Fraud,** the UK's cyber fraud and crime centre.

Abbey Tax
One Mitchell Court
Castle Mound Way
Rugby CV23 0UY
Tel: 0345 223 2727
www.abbeytax.co.uk