

Crime prevention advice for Employees

When it comes to physical and online crime prevention there are several things to consider when it comes to working with your employees. Employees are arguably the greatest asset to a business but can also be working against the businesses. In both instances it is important to consider the following:

Cyber

Education

- It is important to instil good practice, potentially through the use of policies, **put cyber onto the agenda!**
- Potential policies should include: appropriate use of the internet, use of email, regulations on downloading unapproved applications, the use of passwords.
- It would also be useful for a business to stress the importance of reputation and data. Education around the Data Protection Act and other legal obligations would help to affirm the importance of handling data, especially on a computer.
- When it comes to passwords, staff should be advised that they should not be written down, computers should be 'locked' when they are not in use and work space is kept tidy and free of confidential information. This could be contained in a **Computer Usage Policy**.

Beware

- Staff should only have access to information that is relevant to them - consider managing access.
- Something as simple as human error in opening email attachments with a virus embedded could be costly to the businesses systems. It is important to educate employees of the dangers of viruses etc.
- There has been a rise in CEO Impersonation Fraud in which fake emails are sent to employees requesting an invoice to be paid and when they do so, it turns out that the CEO had not ordered this to be done.

Physical

Education

- It is important to inform employees of the physical security onsite so that if they need to implement any of the security measures, they can do so.
- It is important that those members of staff who are responsible for managing security are confident in procedures etc.
- Use strict visitor policies and ensure all staff help implement this.
- Encourage staff to be vigilant and challenge non-employees as to their reasons for being on site.

Beware

- It could be that employees are attempting to defraud the business by stealing stock, money or other assets.
- Disgruntled employees may be assisting others in causing harm to the business, consider access to various parts of the building.
- Keep a regular check that policies and procedures are being followed.

