



BUSINESS WATCH
CRIME REDUCTION ADVICE PACK
for commercial, retail & non-domestic premises

**KEEPING YOUR
PROPERTY & PREMISES SECURE**

SECTION 1 : PREMISES SECURITY

Give Your Business A Security Health Check
10 Minute Security Checklist

SECTION 2 : CRIME REDUCTION

The 25 Techniques Of Business Crime Reduction

SECTION 3 : ALARMS AND CCTV

Types of Alarms & CCTV Systems
Getting The Best From Your CCTV System

SECTION 4 : ADVICE FOR RETAIL PREMISES

Protect Your Shop - A Summary
Prevention Customer Theft - Good Practice Guide

SECTION 5 : PREVENTING METAL THEFT

SECTION 6 : HOW SAFE IS YOUR COMPUTER?

Is Your Computer Safe Online?
How To Avoid Getting Spam
Email Fraud - What To Do
Illegal Or Offensive Material On The Internet

SECTION 7 : PROPERTY MARKING

SECTION 8 : RINGMASTER

SECTION 9 : USEFUL CONTACTS

Revised: MARCH 2009



SECTION 1 : PREMISES SECURITY

TIME TO GIVE YOUR BUSINESS A SECURITY HEALTH CHECK

YOUR BOUNDARIES

- Check fences, walls and hedges for damage and gaps and repair as soon as possible. Prickly plants are a good deterrent and can also be used under vulnerable ground floor windows.
- A low boundary at the front of your property ensures good visibility from passers-by and your neighbours - the Home Office recommend shrubs are cut to a maximum height of 1 metre. If you have trees at the front, make sure branches do not hang lower than 2 metres.
- Your boundary at the back of your property should be approximately 2 metres high. You can increase security by using anti-climb paint or "prickler" strip along the top (with appropriate warning signage). Adding a trellis panel not only increases height but is too fragile to bear body weight, therefore increasing the risk to a burglar.
- Are side entrances secure? Replace any damaged or rusty hinges, hasps and padlocks.
- Good lighting is essential to deter a burglar - consider low level dusk-till-dawn lighting that is cheap to buy and uses less electricity than halogen lamps.
- Consider other warning devices to let you know someone has come onto your property, such as a gravel drive or a driveway alarm.

DOORS

- Check the framework around your external doors (including patio doors and cellar access). It should be securely fixed and in good condition.
- Check the thickness of doors: a door should be at least 44mm if you want to fit a mortise lock - if the door is too thin, then a rim deadlock should be fitted.
- Do you have any wooden panelled doors? Are they strong enough? Often panels are made of a thinner material but these can be easily replaced with something more sturdy.
- Ideally front doors should be secured in two places - usually a mortise lock at a mid-point in the door with a Yale-type latch lock approximately 60-80cm above it. Patio doors should also have bolts that go into the floor and lintel.
- Consider fitting a door viewer, a door chain or bar and even a letterbox cage.
- Does your patio door have suitable frame locks or an anti-lift device? If not, most double-glazing companies can fit these for you.

WINDOWS

- Check the frames of your windows and repair any damage. Pay special attention to those that are vulnerable (ground floor, at the rear of the building, accessible by a flat roof).
- Modern UPVC windows now have locks fitted as standard - British Standard BS7950 - and can be fitted with window restrictors.
- Are the window panes made from laminated glass - this is glass that is extremely difficult to break. Don't confuse laminated glass with toughened glass which is designed for safety.
- Don't forget to check garage/outbuilding windows, especially if the building is attached to the main property with an internal access door.
- Garage and shed windows can be obscured with frosted adhesive vinyl - if a burglar can't see in, it reduces the temptation to break in.

Business Watch

crime reduction advice pack
for non-domestic premises

- You can stop people from climbing onto your flat roofs (and therefore accessing your windows) by painting them with non-drying paint. It is not necessary to do the entire roof but do paint the edges and at least a 2 foot border. Signage must also be displayed.

LOCKS

- Locks are only as good as the screws and framework they are attached to - replace any damaged parts.
- The recommended type of mortise lock is a five-lever lock to British Standard BS3621 / EN12209 (most house insurance policies insist on this specification for the front door).
- If you've got a Yale-style latch lock, is it double locking (ie, if you turn the key, does the block stay in place)? These are more secure, especially if the lock is near a glass panel in the door.
- Mortise bolts operate only from the inside and are suitable for French windows and sliding doors, and are best placed at the top and bottom of the door.

OUTBUILDINGS

- Give your locks and bolts a "health check" - replace any rusty items, ensure all padlocks and hasps bear the British standard kite mark and are made of hardened steel.
- Don't forget the hinges on your doors - if a burglar can't breach the lock, they may attempt to unscrew the hinges. Use coach bolts, non-return screws or simply damage the screw head; you don't need to do every screw, just a couple on the hanging plate and a couple on the door plate.
- Remember to secure outbuilding windows - even the ones that don't open can be vulnerable. Consider obscuring the window with an opaque window film (the type used to obscure bathroom windows) as this will reduce the temptation. Alternatively, fit a grille or a couple of bars across the inside of the window to reduce the window aperture.
- Consider using a battery-operated siren alarm in your garage or shed - they often cost less than £20 and are simple to install and use.
- Get into the good habit of putting everything away when you have finished with it.

GENERAL ADVICE

- Review your cashing up and banking procedures. Make sure you don't get into a habit of going to the bank on the same day at the same time - someone will notice and take advantage of it.
- Ensure your staff are fully aware of their obligations to protect the property, and that they know what to do in an emergency. Would they know who to spot a forged bank note?
- Review the security of your cellars and bottle stores.

These are, of course, only a few ideas to help improve the security of your property.

If you have any questions, please contact the Crime Reduction Office

at Greyfriars Police Station on 01234 275273

or Dunstable Police Station on 01582 473159/473178

10 MINUTE SECURITY CHECKLIST

Below is a checklist to help you to identify the areas where your business may be vulnerable. It is not designed to cover all aspects of security, but will identify some common vulnerabilities.

Tick the appropriate box with your answer. This will help you to establish your business' strengths and weaknesses.

<u>VISITOR ACCESS TO YOUR BUILDING</u>	YES	NO	DON'T KNOW
Are visitors allowed entry to your building by appointment only?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Do they have to report to a reception area before entry?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Are visitors asked for proof of identity?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Are all visitors asked to sign in when they enter the building?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Does your signing in book allow space to note vehicle details?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Are they provided with a visitor's badge?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Are visitor's badges designed to look different to staff badges?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Are all visitor's badges collected from visitors when they leave the building?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Does a member of staff accompany visitors at all times while in the building?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Are the visitor's badges cross-checked against those issued?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Do your staff wear identity badges at all times when in the building?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<u>BUILDING SECURITY</u>	YES	NO	DON'T KNOW
Are there good quality locks on all external doors and ground level windows?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Has all external door furniture been removed from fire doors?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Are there good quality locks on all windows above ground level?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Are any windows above ground level accessible by a flat roof?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Can internal doors be locked when left unattended for long periods?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Are all the fire doors alarmed?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Do you nominate members of staff to check that all doors and windows are closed and locked at the end of the business day?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Business Watch

crime reduction advice pack
for non-domestic premises

If you have a burglar alarm, are your staff familiar with the procedures for switching it on and off (in order to reduce false activation)?

Do you maintain good visibility around the perimeter of your building, eg, cutting back overgrown planting or using palisade fencing instead of panels?

Do you have adequate lighting around your building during the hours of darkness?

CCTV

Do you have your CCTV cameras and recording devices regularly maintained?

Do the CCTV cameras cover the entrances and exits to your building?

Do you have CCTV covering critical areas, such as server rooms or cash offices?

Do you store CCTV images in accordance to the evidential needs of the police?

Could you positively identify an individual from recorded images on your system?

YES NO DON'T KNOW

INFORMATION SECURITY

Do you lock away all business documents at the close of the business day?

Do you have a clear desk policy out of business hours?

Do you close down all computers at the close of the business day?

Are all your computers password protected?

Do you have computer firewall and antivirus software on your computers?

Do you regularly update this protection?

Do you employ the principle of least privilege (where a user be given no more privilege than necessary to perform a job)?

Do you back up business critical information regularly?

Is backed up information stored securely?

YES NO DON'T KNOW

PERSONNEL SECURITY CHECKING

It is important to prove the identity of potential new staff. You should see the original documents, not photocopies, and seek explanations for gaps in information. During recruitment, do you require:

YES NO DON'T KNOW

Full name, date of birth and national insurance number?

Current address and any previous addresses in the last five years?

Business Watch

crime reduction advice pack
for non-domestic premises

- | | | | |
|--|--------------------------|--------------------------|--------------------------|
| Full details of references (names, addresses and contact details)? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Full details of previous employers, including dates of employment? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Proof of relevant educational and professional qualifications? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Proof of permission to work in the UK for non-British or non-European Economic Area (EEA) nationals? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| There is a checklist to establish proof of identity at the end of this document. | | | |

COMMUNICATION

- | | YES | NO | DON'T KNOW |
|--|--------------------------|--------------------------|--------------------------|
| Do you have a security policy or other documentation showing how security procedures should operate within your business? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Is this documentation regularly reviewed and, if necessary, updated? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Do you have a senior manager who takes responsibility for security within your business? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Do you regularly meet with staff and discuss security issues? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Do you encourage staff to raise their concerns about security? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Are you a member of a Business Watch or signed up to a Ringmaster scheme? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Do you know your local Police Beat Manager or Community Support Officer? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Do you speak to neighbouring businesses on issues of security and crime that might affect you all? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Do you remind your staff to be vigilant when travelling to and from work, and to report anything suspicious to the relevant authorities or the police? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

PROOF OF IDENTITY CHECKLIST

It is important to prove the identity of potential new staff. You should see original documents, not photocopies, and seek explanations for gaps in information. The following can assist you in verifying a person's identity:

British Citizens

- | | YES | NO | DON'T KNOW |
|---|--------------------------|--------------------------|--------------------------|
| Do you ask to see, and take a photocopy of, a full and current UK passport? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| If the person does not have a passport, ask to see TWO of the following: | | | |
| British Driving Licence (preferably the photo licence) | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| P45 from previous employer? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Birth Certificate - issued within six weeks of birth? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Credit Card - with three statements and proof of signature? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

Business Watch

crime reduction advice pack
for non-domestic premises

Cheque Book and Bank Card - with three statements and proof of signature?

Proof of Residence - council tax, gas, electricity, water or landline telephone bill?

Other EEA Nationals

Do you ask to see, and take a photocopy of, a full and current EEA passport?

OR a National Identity Card?

Other Nationals

Do you ask to see, and take a photocopy of, a full and current passport?

AND a Home Office document confirming the individual's UK immigration status and permission to work in the UK?

WHAT DO YOUR RESULTS SHOW?

Having completed the checklist, you need to give further attention to the questions that you have answered "no" or "don't know".

If you answered "don't know" to a question, find out more about that particular issue to reassure yourself that this vulnerability is being addressed or needs to be addressed. If you answered "no" to any question then you need to address that particular vulnerability as soon as possible.

Where you have answered "yes" to a question, remember to regularly review your security needs to make sure your security measures are fit for purpose.

SECTION 2 : CRIME REDUCTION

The 25 Techniques Of Business Crime Reduction SOME IDEAS TO HELP YOU TO TACKLE CRIME

INCREASE THE EFFORT	INCREASE THE RISKS	REDUCE THE REWARDS	REDUCE PROVOCATION	REMOVE THE EXCUSES
1 HARDEN TARGETS <ul style="list-style-type: none"> ◆ Secure the perimeter ◆ Secure the building ◆ Anti-robbery screens 	6 EXTEND GUARDIANSHIP <ul style="list-style-type: none"> ◆ Town centre and shopwatch schemes ◆ Improve communications 	11 CONCEAL TARGETS <ul style="list-style-type: none"> ◆ Reflective film ◆ Window blinds 	16 REDUCE FRUSTRATION AND STRESS <ul style="list-style-type: none"> ◆ Clear tills regularly ◆ Efficient queuing ◆ Staff training 	21 SET RULES <ul style="list-style-type: none"> ◆ Clear rental agreements ◆ Staff security policy
2 CONTROL ACCESS TO FACILITIES <ul style="list-style-type: none"> ◆ Gates on alleyways ◆ Single entry point ◆ Security cabinets 	7 ASSIST NATURAL SURVEILLANCE <ul style="list-style-type: none"> ◆ Control growth of trees and bushes ◆ Improved external lighting 	12 REMOVE TARGETS <ul style="list-style-type: none"> ◆ Reduce amount of cash on premises ◆ Secure stock areas ◆ Remove stock 	17 AVOID DISPUTES <ul style="list-style-type: none"> ◆ Display fixed tariffs ◆ Reduce crowding in pubs 	22 POST INSTRUCTIONS <ul style="list-style-type: none"> ◆ "No Parking" ◆ "Private Property" ◆ "Please ask for assistance"
3 SCREEN EXITS <ul style="list-style-type: none"> ◆ Put tills near the exit ◆ Electronic tags for stock ◆ Staffed reception 	8 REDUCE ANONYMITY <ul style="list-style-type: none"> ◆ Staff/visitor IDs ◆ "How's my driving?" signs ◆ "Can I help you?" ◆ Visitor sign-in books 	13 IDENTIFY PROPERTY <ul style="list-style-type: none"> ◆ Security marking ◆ Tagging assets ◆ Asset and stock lists 	18 REDUCE EMOTIONAL REACTION <ul style="list-style-type: none"> ◆ Control sexual and violent imagery ◆ Remove fur items from windows 	23 ALERT CONSCIENCE <ul style="list-style-type: none"> ◆ "Shoplifting IS Stealing" ◆ Log-in screen on computers ◆ Proof of age reminder
4 DEFLECT OFFENDERS <ul style="list-style-type: none"> ◆ Secure access roads on industrial estates ◆ Town centre patrols 	9 UTILISED PLACE MANAGERS <ul style="list-style-type: none"> ◆ Train employees to prevent crime ◆ Support whistleblowers 	14 DISRUPT MARKETS <ul style="list-style-type: none"> ◆ Identify stock and assets ◆ Communication between traders 	19 NEUTRALISE PEER PRESSURE <ul style="list-style-type: none"> ◆ Prosecute shoplifters ◆ "It's OK to say No!" 	24 ASSIST COMPLIANCE <ul style="list-style-type: none"> ◆ Approach all customers ◆ Litter bins ◆ Public lavatories
5 CONTROL TOOLS AND WEAPONS <ul style="list-style-type: none"> ◆ Secure displays of tools, welding gear, etc ◆ Metal detectors 	10 STRENGTHEN FORMAL SURVEILLANCE <ul style="list-style-type: none"> ◆ Security guards ◆ Monitored CCTV system 	15 DENY BENEFITS <ul style="list-style-type: none"> ◆ Banknote staining ◆ Ink-tag merchandise ◆ PIN codes 	20 DISCOURAGE IMITATION <ul style="list-style-type: none"> ◆ Repair vandalism ◆ Security chips in electrical equipment 	25 CONTROL DRUGS AND ALCOHOL <ul style="list-style-type: none"> ◆ Breathalysers/drug itemisers in pubs ◆ Alcohol-free events

SECTION 3 : ALARMS AND CCTV

GUIDANCE FOR COMMERCIAL PREMISES

It is always difficult to give advice without visiting the site, as most often the remedies are site specific. Before we go further, it should be pointed out that Bedfordshire Police are not permitted to recommend or endorse products, services or suppliers.

However, there will be circumstances where perhaps there is only one manufacturer or supplier of a particular product and it is unreasonable to tell somebody about a product that could solve their problem but refuse to tell them where to get it from. Where possible, we will provide a couple of sources that you can investigate for yourself.

Those companies and products mentioned in this document are used because they are locally available, represent value for money as well as good practice and have, to date, generated no negative reports in our experience.

BURGLAR ALARMS

Alarms come in various forms and the homeowner's requirements will depend on factors such as how remote their home is and how responsive the neighbours would be to an alarm activation.

Alarm companies such as ADT and (locally) ACE are reputable and have reputations for not trying to sell you a product or additional services you don't need.

These, and many other alarm companies, can provide a monitoring and police reporting service as well as service and maintenance. All of this does, of course, cost money and, should the homeowner decide to have such a system fitted, they would be well advised to have two or three quotes for both price and service comparison.

Trading Standards may also have a list of reputable traders and can be contacted on 01234 228280 or view their listings at www.bedfordshire.gov.uk/tsapproved.

Alarm companies can also be registered with the National Security Inspectorate. You can check if a firm is registered by visiting www.nsi.org.uk.

There are also many DIY systems that can be fitted by a reasonably competent person and not requiring an in depth electrical knowledge. There are also a number of battery-operated, wirefree, systems on the market.

These are an economical option and whilst there is not the services of a monitoring company, some such systems will contact telephone points - including mobiles - of choice (eg, the Yale wire free alarm kit, currently available from Homebase at £249, which will contact up to 6 phone numbers; Micromark do various systems starting from around £80 to £250).

Most DIY stores supply alarms, as do the Argos and Littlewoods catalogues. Look for the British Standards Kite mark BS6707.

Another DIY alarm manufacturer is Micromark (who also make home CCTV cameras). It is worth looking at their websites: www.micromark.co.uk. You can also look at : www.yale.co.uk

CCTV SYSTEMS

CCTV often unrealistically raises expectations and it is important that you realise the limitations of any camera. At its best, for example town centre CCTV, an operator can focus and zoom in or out to obtain the best 'product' image. Realistically the type of camera you attach to your home will be

Business Watch

crime reduction advice pack
for non-domestic premises

of a fixed focal length and so the positioning of the camera, to obtain best possible facial recognition, is the priority.

Systems can be plugged straight into the TV or VCR without expert knowledge and, as most have integral PIR sensors, will switch on your TV or VCR from standby mode, if activated or switch channels automatically so that you are immediately made aware of a 'visitor'.

You should consider the amount of time you can cover on a tape. Most domestic VCRs, with long play mode, can record for 8 hours but continuous recording will wear the heads and you might consider a more robust machine. Generally a domestic model will suffice, especially as you can replace them for around £30-£40 these days. Check your tapes regularly and change them before the recorded product deteriorates too far.

There are restrictions on what and where you can record and there are implications under the Data Protection Act to name but one. There are exceptions for Crime Reduction and Personal Safety purposes, particularly in domestic applications. Care should be taken not to intrude onto adjacent properties and any recorded material should not be readily available or viewed to a wider audience as entertainment. Indeed, in the event that an offence is recorded, the integrity of the evidence can be best preserved by the restriction of viewing to the owner (yourself) and any investigating body, ie, the police.

Cameras are available from most DIY stores, catalogues and on the Internet.

AND FINALLY...

Bedfordshire Police are only able to give an opinion on what measures might reduce crime and there can be no guarantee that such measures will prevent crime. Crime Prevention advice is given free without the intention of creating a contract. Neither the Home Office nor the Police Service therefore takes any legal responsibility for the advice given.

We are sure you will appreciate that the above is by no means exhaustive and may not include every possible aspect of security. However, should you feel that the Crime Reduction Officers can be of any further assistance, please do not hesitate to contact us.

We hope that the above is helpful to you and we would be grateful to be kept informed of any measures implemented.

North Bedfordshire: Lara Curtayne & Pete Spicer 01234 275273

Mid & South Bedfordshire: Lesley Johnson & John Shiels 01582 473159/78

GETTING THE BEST FROM YOUR CCTV SYSTEM

How many times have you watch fuzzy, poor quality images on television of offenders committing a crime or disorder and not been able to identify anyone?

More and more businesses are investing in CCTV systems to help prevent and detect crime, but all too often, the images they capture are poor quality and of little evidential value. This poor quality can result in many images being rejected before they reach court.

If you've invested large sums of money in a CCTV system, it's simply a waste not to use it in the most effective way possible. It may also be unlawful.

If you want to protect your premises and bring offenders to justice, Bedfordshire Police have prepared this advice sheet to help you when buying, installing and using CCTV.

TOP TIPS FOR TOP PICS

- Make sure cameras are positioned correctly and are in focus. For example, you cannot identify anyone if all you can see is the top of their head.
- If you have a number of cameras, think about the area they are covering. Do they really need to cover wide open areas which mainly cover shots of a ceiling or a wall?
- Think about installing a camera at your main front door, showing people entering and leaving the premises. No matter how quickly they are moving, everyone has to stop for a few seconds to open a door – long enough to get a good picture.
- If it's fixed camera, is it balanced properly to give good quality images?
- Regularly check the time and date on your system and take into account changes such as British Summer Time.
- Arrange a regular maintenance contract to have your CCTV system cleaned and serviced – don't forget to include any recording equipment.
- In between services, carry out your own "spring cleaning" by making sure lenses and the heads on any video recording equipment are clean.
- If using VHS systems, make sure you buy good quality tapes. Change and rotate tapes regularly. You must keep the images for the period you stated when notifying the Data Commissioner and no longer. Store video tapes in an upright position in a clean and secure location, away from heat and humidity. Label all tapes and discs clearly. Tape management systems are available to help keep your system lawful.
- Have signs clearly displayed around your premises stating CCTV is in use and its purpose.
- Remember, if in doubt, contact your CCTV provider for advice on how to improve your system

DO:

- ensure your system has been notified to the Data Commissioner.
- make a benchmark tape when you first install the system to compare against future images to ensure quality.
- change your video tapes at least every week and check the time and date stamps are correct
- ensure your tapes are kept for the appropriate period of time that you notified to the Commissioners Office.
- use good quality tapes and check them by playing them on a different machine.
- ensure the picture is clear enough to identify people and vehicles.
- check the cameras are covering the most effective areas.
- make sure the lighting is sufficient to capture a good picture without being so bright as to cause "flare" on the image.

DON'T:

- continually re-use the same tapes – the quality of image will become progressively poorer.
- let the tapes get dirty or expose them to heat or humidity.
- place the tapes near a magnetic field, eg, loud speakers.
- touch the video tape itself.
- buy cheap, inferior video tapes.
- use 240 minute tapes.
- record in long-play.
- have a viewing angle that is too wide.
- use video tapes more than 12 times.

UK POLICE REQUIREMENTS FOR DIGITAL CCTV SYSTEMS

QUALITY:

What Resolution? What Compression?
How Many Pictures Per Second?

- Specify your requirement - decide what you want to see and where, and select a system that will do it.
- View the recorded pictures or print out to check quality - don't rely on the live screen to assess the system performance.
- The system clock should be set correctly and maintained (taking account of GMT and BST).
- Picture quality should not be reduced to fit the available storage capacity of the system.
- Regular maintenance should be conducted on all aspects of the system.

STORAGE:

What Should I Keep?
How Should I Keep It?

- The system should be operated and recorded pictures retained in secure environment.
- Electronic access controls, such as passwords or encryption, should not prevent authorised access to the systems or recordings.
- The system should have sufficient storage capacity for 31 days' good quality pictures.
- The system should be capable of securing relevant pictures for review or export at a later date.

EXPORT:

How Much Video Should The System Export
And In What Format?

- A system operator should be available who is able to replay and export recordings.
- A simple system operator's manual should be available locally to assist with replay and export.
- The operator should know the retention period of the system and export time for various amounts of data.
- The system should be able to quickly export video and stills to a removable storage medium, with time and date integral to the relevant picture.
- Export should include any software needed to view or replay the pictures.
- The system should have an export method proportionate to the storage capacity.
- Pictures should be exported in the native file format at the same quality that they were stored on the system.

PLAYBACK:

Can The Pictures Be Easily Viewed By
Authorised Third Parties?

- The playback software should:
 - have variable speed control including frame-by-frame, forward and reverse viewing;
 - display single and multiple cameras and maintain aspect ratio, ie, the same relative height and width;
 - display a single camera at full resolution;
 - permit the recording from each camera to be searched by time and date;
 - allow printing and/or saving (eg, bitmap) of pictures with time and date.
- The time and date associated with each picture should be legible.
- Once exported to removable media, it should be possible to replay the files immediately.

SECTION 4 : ADVICE FOR RETAIL PREMISES

PROTECT YOUR SHOP - SUMMARY

Remember to **KEEP SAFE**. Your safety is worth more than your property.

If you find yourself in an aggressive or violent situation don't take any risks. Your personal safety comes first. These approaches may help you:

- Watch out for warning signals such as hostile body language, nervousness or smell of alcohol.
- Avoid actions that may trigger violence such as standing too close to people, pointing, touching, turning your back, swearing or making sudden movements.
- Keep calm and behave as normally as possible.
- Keep your distance from threatening behaviour. Get behind the counter and don't get involved in an argument.
- Get help. Have arrangements to call for support and use them.
- Make a note of all incidents.
- Remember the offender's distinguishing features.

Remember you have a right to refuse to let anyone who is acting criminally, or who is offensive, into your shop.

STAFF AWARENESS

Making sure your staff are confident, alert and well informed is the best way of preventing crime. You can train your staff while they are doing the job.

- Be aware for suspicious behaviour, out of character shoppers or customers distracting staff.
- Set up store procedures for recording crime incidents such as when to call the police, how to handle cash and how to use security equipment.
- Keep safe and don't take personal risks. Pick up warning signals and use techniques for preventing aggression.
- Prevent fraud by routinely checking credit and debit cards in line with guidance from card issuers. Check bank notes for forgery.

Good customer care can put off thieves and prevent tense situations.

STORE DESIGN AND LAYOUT

- Make it easy to see and be seen. Keep shelves low enough for staff to see what shoppers are doing. Use mirrors to reduce blind spots. Make it easy to see into your shop from the street.
- Provide staff with safe spaces such as counters, with gates or doors that can be closed to prevent unauthorised access.
- Protect high value goods. Display them away from exits and where you can see them.

WORK SAFE - WORK SMART

- Avoid lone working.
- Get experienced staff to work with inexperienced staff.

Business Watch

crime reduction advice pack
for non-domestic premises

- Lock up property. Make it clear who is responsible for locking windows, doors, cabinets and for setting alarms.
- Handle cash with care. Do not keep large amounts of money in your till. Vary routine if you are going to bank.
- Take care when you recruit. Get character references.
- Limit the number of staff who have keys to your store.
- Record all incidents of crime. This will help you spot trends or patterns and will help the police if you have to call them.
- Review your measures for fraud prevention. Make sure that staff know about point of sale checks and bank reward schemes for detecting stolen debit/credit cards.
- Control stock tightly and limit access to it.

DON'T DISCOUNT CRIME

Preventing crime pays. Businesses are more at risk of crime than private households. Reducing the risk of crime will help protect your profits and make sure that the people who work with you are safe. Everyone needs to play a part in tackling crime effectively.

Whatever you decide:

- Do several things. Don't rely on just one solution.
- Involve everyone who works in your store and use their experience
- Remember partnership pays! You'll be able to do more by working with others.

Put yourself in the shoes of a criminal and think how you would be able to steal from your shop and act on it to prevent it from happening.

PREVENTING CUSTOMER THEFT – GOOD PRACTICE GUIDE

This guide provides information on how to deal more effectively with customer theft - shoplifting. Customer theft is very widespread and is often dismissed as minor crime. The advice contained in this booklet will help to reduce the impact of shoplifting - and since it is very likely that you will confront a shoplifter at some time, let us begin with the legal definition of theft.

WHAT IS THEFT?

The Theft Act, 1968 says that: a person who dishonestly takes property belonging to another, with the intention of permanently depriving the other of that property, is guilty of theft.

The Main Types Of Customer Theft In Shops

OPPORTUNISTS

Many shop thieves are not regular offenders, but may be influenced by the opportunity that presents itself to them at the time. Retailers should try to ensure that expensive items do not present easy targets. Thieves may steal on a daily or weekly basis, may be regular or longstanding customers and may mix purchases with stolen goods. It is prudent not to take anyone for granted. It will be difficult to prevent thieves stealing many smaller and less expensive items that are on open display - food, clothing, confectionery, cosmetics etc.

JUVENILES

Young people can be influenced by pressure from school or friends to join in stealing. They may also be bullied or coerced into stealing. Groups of young people can present a particular problem and retailers need to try and manage them, perhaps by limiting numbers allowed into the store, insisting on an adult accompanying them or by excluding them at certain times - lunch breaks and after school. Plastic screens in front of confectionery displays can reduce the opportunity to steal.

THIEVES WHO USE CHILDREN

Some people use children either to carry out thefts or to disguise adults stealing. Babies (both real and dolls) in prams can be used as decoys and to hide goods. Goods may be given to young children to walk out of the store with or they may be placed on the under-tray of the pram.

MENTALLY ILL OR DISTURBED PERSONS

A very small number of people who steal may suffer from a compulsive condition. Other persons who steal may be suffering from other forms of mental ill health and retailers should always be conscious of the possibility that someone they are dealing with falls into this category. Some elderly people may be confused or forgetful and it may be appropriate to either offer to help them when they enter your store or see if there are friends or relatives who can accompany the person so as to prevent misunderstandings.

DRUG ABUSERS

The single biggest problem for retailers is that of drug abusers who steal to support their addiction. They are persistent and may try to steal repeatedly on the same day. They should always be refused entry to the store or escorted from the shop if found inside. It is safer to do this than to try and detain them once they have stolen goods, as their behaviour may become irrational or violent if their freedom is challenged.

DISTRACTION THEFT

This is a method where a group of people will enter a store and distract staff in order to steal either bulk items, or expensive goods. In many cases, retailers will be unaware that they have been victims until later. Some younger groups of distraction thieves may create a disturbance and become violent if challenged.

STAFF COLLUSION

All retailers (and other businesses) are at risk of collusive fraud and theft of goods and cash between staff and customers. Sometimes staff will willingly work with friends or relatives or they may be coerced into doing this. Frequent till checks, strict compliance with till procedures and personal or CCTV observation of suspected collusive staff will help to reduce opportunity and set the standard.

PROFESSIONAL THIEVES

The increasing number of thieves who travel locally, regionally or nationally to steal from shops several times a day, every day of the week is a growing and serious risk. They will steal large

Business Watch

crime reduction advice pack
for non-domestic premises

quantities of goods, mainly of high value, frequently work in groups and may resort to violence if caught. Retailers may not be aware that they have been visited until they discover their losses.

What Can You do About It?

Not all of the following practical suggestions will apply to your business. The level of shop theft committed against your premises will depend on a range of factors. These include:

- the type of goods you sell
- the location
- the layout of your shop and the style and location of your displays
- the local crime rate
- the hours you trade
- the number of staff you employ and their experience

You need to consider all of your circumstances and then choose the preventive measures that suit you best. Your local crime prevention officer will help you do this. Remember - all retailers are at risk. Never think that your type of business isn't.

ESTABLISH A POLICY

Establish a store policy for the prevention of customer theft and ensure that all staff are aware of it. Remember to brief new and part time employees on store policy and procedures.

TRAIN YOUR STAFF

Well trained and alert staff form the basis for good crime prevention. Don't rely on technology instead of investing in proper staff training. Get advice from the Business Crime Reduction Partnership, crime reduction officer, trade association or trade newspaper. Training need not be expensive - 15 minutes each week should be enough to refresh your staff's memories, and stay alert.

BE VIGILANT

Teach your staff to be alert, and to recognise shop thieves. Thieves will often look around the room rather than at the products, or behave in other suspicious ways. Train your staff to spot potential thieves.

DETER OFFENDERS

The most effective - and cost-effective - way to prevent shoplifting is to deter known offenders by declining to let them enter your store, or politely asking them to leave if they have gained entry. This reduces the risk of violence, which can occur if an arrest has to be made and lets the person know you are alert and aware (see Store Banning).

KNOW WHAT TO DO

Decide what you expect your staff to do when a suspect is identified. Making suspects aware they have been noticed will often be enough to deter crime. Use the normal sales approach, eg, 'can I help you in any way?' or 'can I help you find anything?' Make yourself busy near the suspect; keep

walking past them; smile at them, and look them in the eye. If the theft has already occurred you will want your staff to keep the suspect under observation - or alert specialist security staff if you employ them - with a view to making an arrest - see 'Making Arrests' Good Practice Guide.

Physical Security

Use a combination of preventive measures. Most strategies work best in combination rather than in isolation, eg, CCTV can work effectively, particularly where helped by security mirrors, good lighting, and alert well trained staff. Store design is important. Ask your crime prevention officer to advise you. Some useful measures are:

DUMMY DISPLAY GOODS

Empty display boxes or disabled products can help to reduce theft of electrical goods, music or other high risk or small items.

SECURITY CABINETS

High value goods can be displayed in lockable glass cabinets but, they must be of a good quality, with doors that are not able to be lifted out, with good quality locks and strictly controlled access to keys.

WARNING NOTICES

Signs advertising the presence of recorded CCTV, central station alarms, hold-up alarms or the store till and cash policy (no cash left on premises) can play a part in deterring potential thieves, burglars or robbers.

MIRRORS

Mirrors can help you keep an eye on areas that would otherwise be out of sight.

DISPLAY (LOOP) ALARMS AND TAGGING

High value goods can be protected by alarm wires which 'loop' through them to an alarm box. If the wire is disconnected or cut, the alarm sounds. Product tagging may also be of value.

STORE BANNING

Shops are private property with an implied invitation to enter to purchase or browse. A retailer can ban a person from a shop if his/her presence is not conducive to the business. This will include people who are violent, threatening or abusive, drunk or under the influence of drugs, or who are known or strongly believed to be involved in theft. A person who is banned should be told only that his/her presence is not wanted and that they should shop elsewhere. Do not become involved in giving detailed reasons for your actions.

Working With Others Business Crime Reduction Partnerships

There are over 200 business crime reduction partnerships (BCRPs) in towns and cities helping to reduce business crime and violence. They operate as membership organisations and link businesses, mainly retailers, through radio links so members can be aware of current criminal activity. The radios are frequently also linked to the local town CCTV, police and other agencies such as wardens. They also share photographs and other information about known thieves and operate partnership exclusion schemes whereby known thieves and anti-social persons are excluded from the premises of all the members.

These partnerships are very successful in deterring known and prolific thieves from members' stores and reducing the incidence of crime, abuse and violence. BCRPs are an important part of the local community safety plan and work closely with other organisations and agencies to ensure that business crime continues to be seen as a key issue for community safety.

HOW TO JOIN

For more information on whether there is a BCRP in your area go to the Action Against Business Crime (AABC) web site: www.businesscrime.org.uk and click on 'crime partnerships' then telephone or e-mail AABC for further details. The web site contains much information about the work of AABC, so please take some time to see what is being done to support businesses in their fight against crime and see how you can make an active contribution by joining your local BCRP.

SECTION 5 : PREVENTING METAL THEFT

The increase in metal theft is being put down to the massive price rises in the cost of raw materials including lead, copper and zinc. Thefts are not just from building sites and farms, but also a growing number of cabling companies and electrical sub-stations. The roofs of churches and schools are also being targeted.

There are products on the market that can be used to property mark metal - these are some suggestions:

- SELECTADNA Grease for outdoor applications. The grease is impregnated with UV tracer and a unique DNA code, linking the criminal to the crime scene. It is also easy to paint on all lead roofing, copper pipes and cables.
- SMARTWATER is appropriate for sheet metals before processing. Many companies store raw metals in their premises in readiness for production of other items. Spraying the sheets with Smartwater and displaying signage will act as a deterrent.
- UV PEN MARKING is appropriate for plumbing and heating products. Many builders and developers leave boilers, pipes and radiators in unoccupied premises overnight. Marking them with the site details and leaving a sign in the window may help to deter theft.

RINGMASTER

Signing up to our RINGMASTER system will alert you to current metal thefts in your area or connected to your business. You will find the form in Section 8 of this document.

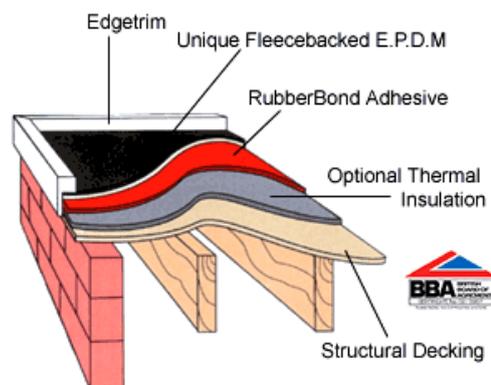
PLACES OF WORSHIP

Bedfordshire Police are developing a pilot scheme called "FaithWatch". It works in a similar way to Neighbourhood Watch and Business Watch, and will use Ringmaster as it's main way of communication. You will soon see these signs around the county.



ALTERNATIVE PRODUCTS

It is worth considering replacing lead sheeting with Rubberbond EPDM (Ethylene Propylene Diene Monomer). More information about this product can be found at www.rubberbond.co.uk and there are a number of certified installers in the area.



SECTION 6 : HOW SAFE IS YOUR COMPUTER?

IS YOUR COMPUTER SAFE ONLINE?

Please read this document if you use the Internet. The risk to you is low but it's worth spending a few minutes to make yourself aware of how you can be vulnerable when online.

Your computer operates under an "open door" policy. Bank account details, passwords, credit card numbers, documents and other personal information that you don't want to share with the world - they are all available to anyone else on the Internet. You probably have no idea that all the time you are online, computers all over the world have a look at your computer with hits every couple of minutes!

- Hackers can get in, take what they want and even leave open a "back door" so they can access your computer anytime you're online and use it to attack other computers.
- Advertisers and other web sites spy on your Internet habits by placing cookies (small files that external web sites place on your computer) which then report that information, usually without your knowledge, to the cookie owner.
- Anti-virus software does nothing to secure your computer against direct attacks. Most people think it protects them completely from Internet-borne threats but virus protection is only as good as the latest virus definitions, which are created in response to the newest viruses. Someone (potentially many thousands of people) must be infected before the makers of anti-virus software can create a defence.

YOU NEED A PERSONAL FIREWALL

In buildings, a firewall is a barrier that prevents a fire from spreading. In computers, the concept is similar. There are a variety of "fires" out there on the Internet: hacker activity, viruses, unwanted cookies and so forth. A firewall is a system that stops the "fire" from spreading to your computer.

A firewall guards the "doors" to your computer - the ports through which Internet traffic comes in and goes out. The firewall only lets traffic through the ports that you have specified to be used. Each port is specifically numbered. For example, Port 80 allows browsing on web pages, Port 1863 allows Instant Messaging, Port 443 allows access to secure web pages used by online merchants to encrypt purchases.

A firewall has three security benefits:

- No one can sneak into your computer through an unguarded port.
- Programs on your computer can't use unguarded ports to contact the outside world without your permission.
- Spam emailers can't "see" your computer so easily.

A firewall is a piece of software that monitors all incoming network traffic and allows in only the connections that are known and trusted. Firewall software also takes away the burden of granting or restricting access to the some 65,000 ports available on your computer. In general, it will restrict access to the majority and you have to grant permission to open the port. The fewer ports you have open, the more "invisible" your computer is on the Internet making it less at risk.

More advanced firewall software also monitors outgoing traffic. This is crucial as you may unknowingly pass on a virus to a contact.

HOW DOES A FIREWALL WORK?

All Internet traffic - web pages, email, audio files and so on - are transmitted in bite-sized chunks called "packets". Each packet is addressed to a particular computer and to a particular port on that computer. The computer "baddies" out there like to send malicious packets with destructive capabilities. A firewall examines every packet that arrives at your computer and asks four questions:

1. Where did it come from?
2. What port is it addressed to?
3. Does the rules allow traffic through that port?
4. Are there any other rules the packet violates?

If the firewall gets a wrong or unsatisfactory answer to any of these questions, the packet is blocked.

PORT SCANNERS

Port scanning is a technique hackers use to find unprotected computers on the Internet. Using automated tools, the hacker systematically scans the ports on all the computers in a range of IP addresses, looking for unprotected or "open" ports. Once an open port is detected, the hacker can then use it as an access point to break into the unprotected computer.

WHY DO I NEED PROGRAM CONTROL?

Everything you do on the Internet - from browsing web pages to downloading MP3 files - is managed by specific applications (programs) on your computer. Hackers exploit this fact by planting "malware" (literally, evil software) on your computer. Sometimes, malware is sent as an email attachment with an innocent name such as "screensaver.exe" and, if you open the attachment, the malware installs itself onto your computer without you even knowing it. Another way malware can get onto your machine is via a message saying you need to upgrade a legitimate program on your computer.

Once on your computer, malware can cause havoc. It can access your address book and send itself to all your contacts, or wait for you to connect to the Internet again and send itself back out onto the web. You risk losing all your programs and stored data, and even making your computer unredeemable.

Program control searches for malware and prevents it from being launched on your computer.

WHY DO I NEED COOKIE CONTROL?

Cookie control keeps advertisers from spying on your Internet habits. High security settings keep sensitive information (passwords, for example) from being stored in cookies, where they can be stolen if a hacker breaks into your computer.

- **Persistent Cookies:** a cookie that stays on your computer a long time and lets the web site remember who you are and what you look at so that the next time you visit that site, it can customize what you see. For example, this is how Amazon shows you books that you may be interested in each time you visit.

- **Third-Party Cookies:** placed by someone other than the web site host and can be used to record information about your Internet habits. For example, which advertisements you click on.
- **Session Cookies:** a cookie stored in your browser's memory cache that disappears as soon as you close your browser. These are the safest cookies because of their short lifespan.

Medium cookie control setting allows session cookies and persistent cookies but blocks third-party cookies. This protects you from information leaks while preserving the convenient function of cookies.

WHY DO I NEED ADVERT CONTROL?

Ad blocking keeps unwanted advertisements from disrupting your Internet work. With a firewall you can block all types of adverts or only specific types.

- **Banner and skyscraper adverts** extend across the top or up the side of the web page itself. They are built into the web page so cannot be removed but it is possible to block the content. This is called performance ad blocking and keeps adverts from slowing down your Internet access.
- **Pop-up and pop-under adverts** appear in a new browser window that "pops" up in front of or under the screen you are looking at. A firewall can block pop-up and pop-under ads as if they don't exist.

THE PROBLEM WITH EMAIL ATTACHMENTS

Attaching files to email messages is a convenient way of exchanging information. However, it also provides hackers with an easy way of spreading viruses, worms, Trojan horse programs and other malware.

It's never a good idea to open an email attachment you weren't expecting unless you know the person it came from and have confirmed (by telephone or separate email message) that that person actually sent it to you. Remember, hackers can alter a message to look like it came from a trusted source.

WHERE CAN I GET A PERSONAL FIREWALL?

As with all software, it's a matter of personal choice as to what product you use. Do your research on the Internet before buying a package but here are some of the more popular brands on the market:

- **Zone Alarm:** www.zonelabs.com
- **McAfee Firewall:** www.mcafee.com
- **Norton Personal Firewall:** www.symantec.com

HOW TO AVOID GETTING SPAM

Simple precautions and software can dramatically reduce the amount of spam you get. Find out how to stop those endless invitations to lose weight, donate money, buy pharmaceutical products or subscribe to special (usually adult) services.

WHY YOU GET SPAM

The Internet holds millions of email addresses, irresistible to salesmen. Because the Internet is so vast and email is cheap or even free, there is little incentive for spammers to narrow down their mailing lists. A child in Aberdeen can receive the same advert as a pensioner in Southampton.

WHAT NOT TO DO

Don't act too fast - some responses might just make matters worse. Here are some golden rules:

- Don't reply - ever!
- Never buy anything from a spammer. If they know you are willing to buy, you will be bombarded with more spam.
- Think twice before forwarding chain letters or petitions. Mass mailings like this constitute spam and the lists of addresses on them are later use by spammers.
- Don't "mail bomb" the spammer who seems to have singled you out. The address included in the email is probably forged from an innocent person's account or belongs to a mailbox the spammer never visits.

HOW THEY FIND YOU

People find they get spam once they:

- Post a message on a newsgroup.
- Give their email address to an online retailer.
- Sign up for an Internet service that requests an email address.
- Email a spammer asking them to remove their address from the mailing list.

Unfortunately, once you're on a spam list, it's very hard to get off but avoiding these traps may help you to reduce the amount of spam you get.

FIRST STEPS

- Now you know how valuable your email address is, think about whether the sites that ask for it really need it.
- You can always "accidentally" misspell your email address when you register. The only problem with this is some sites insist on sending an email with your password to get into the site.
- You might want to set up an email account solely for the purpose of joining newsgroups, forums and buying online.
- Using a free-mail account like Yahoo, Hotmail, or Lycos (to name a few) to deal with special accounts will attract the spam away from your personal email accounts.

PREVIEW

More advanced spammers put tiny invisible images into their emails that are stored a main website. That means when you look at an email using the preview feature (where you see the first few lines of a message), your email program visits the site to download the images. Accessing these pictures tells the web site that your email account is active and worth sending more spam to. It's a good idea to turn off the preview feature and only open emails where you know the sender.

BLOCKING SPAM FEATURES

Your free-mail or personal email program probably already has an integrated basic spam filter. This will move suspected spam into a separate folder until you are ready to check it. Some programs also allow you to specify which emails can be deleted before they are even delivered to your Inbox.

ANTI-SPAM PROGRAMS

If your email program or free-mail account cannot deal with the spam you are getting, you could try a dedicated anti-spam program. These automatically junk suspect emails either on your server or on your computer. Mailwasher, McAfee Spamkiller, Mailfrontier Matador, Cloudmark Spamnet and SpamBully are just a few of the programs that do this.

By filtering your email, the program builds a "blacklist" of spam addresses and automatically deletes them when further messages arrive from the same address. Some programs also look for clues in the email heading - for example, "xxx" or "buy online".

CHOOSING THE RIGHT PROGRAM

These are some things to think about when choosing an anti-spam program:

- Does the program check for spam before or after downloading?
- Does the program integrate into your email program or is it stand-alone?
- Does it work with your existing set up? (Some programs will only work with certain email programs, such as Outlook or Outlook Express, or certain freemail accounts.)
- Does it keep filtered mail for later retrieval?
- Check out CNET and Zdnet for lists of more spam blockers.

YOUR INTERNET SERVICE PROVIDER (ISP)

Your ISP may be able to block spam at its gates before it even reaches your mailbox. Ask them what services they offer. If they do not make this provision, think about changing ISPs. It could save time and money.

EMAIL FRAUD – WHAT TO DO

Unfortunately, one of the hazards of email is the unwanted mail delivered daily to our Inboxes. There have been a number of incidents reported nationally regarding fraudulent emails which aim to relieve a person of vast amounts of money by offering fantastic overseas financial schemes and promising great returns through investment.

As plausible as some of these schemes sound, our advice is **DON'T FALL FOR IT!**

All it takes is one person to respond to these emails to make the whole exercise worthwhile to the offender.

- Do not reply to these emails in the first instance - once they get hold of you, they are very difficult to shake off.
- Do not send any money or submit your bank details under any circumstances - even if you have been promised a large cash prize.

- If the sender's email address ends in an ISP name, send a copy to the ISP of the sender using "abuse@...". (eg, abuse@hotmail.com, abuse@yahoo.co.uk, etc). This will alert the ISP that they are being used in fraudulent activity.

THE "419" ADVANCED FEE FRAUD

The National Criminal Intelligence Service (NCIS) issue constant warnings for people to be on their guard against a surge in fraudulent emails promising large cash payouts in exchange for a small upfront investment, commonly known as '419' Advanced Fee Fraud. Churches and charities have also been targeted.

A business or individual receives an email from an 'official' allegedly in a foreign government or agency. An offer is made to transfer millions of pounds - for reasons including paper currency conversion, real estate ventures, business investment, a legacy or simple fraud - into your personal bank account. You are encouraged to travel overseas to complete the transaction and sent documents with official-looking seals and logos testifying to the proposal's authenticity. Throughout the fraud, you are asked to provide advance fees for taxes, legal fees, transaction fees or bribes.

EMAIL "PHISHING" SCAMS

Some people may have received fraudulent emails asking them to confirm information such as Internet banking or telephone banking User IDs, Passwords and Memorable Information. These are not genuine emails and this activity is known as "phishing".

If you receive such an email, please do not click on any link or provide any Internet banking or telephone banking log on details. While your bank may send you emails from time to time, they will never send emails asking for your Internet banking information. For a quick way to tell if an email is genuine, check for your name at the top of the email. Your bank knows who you are so they'll always greet you personally, but fraudsters are unlikely to know your name.

The aim of many email scams is to lead you to websites that may look like an official bank web site but are in fact 'spoof' sites.

If you receive an email saying you need to re-activate an account, please send it directly to the bank the email is supposed to have come from, and then delete it from your Inbox.

Some useful contact details to report "phishing" are:

- **Barclays Bank:** internetsecurity@barclays.co.uk.
- **Lloyds TSB:** emailscams@lloydstsb.co.uk
- **HSBC:** 0845 600 2290
- **Nationwide:** phishing@nationwide.co.uk
- **NatWest:** nwoib@natwest.com

ILLEGAL OR OFFENSIVE MATERIAL ON THE INTERNET

British Police can only take action where material falls within their jurisdiction, ie, within the UK. It often happens that offensive web sites report to British Police turn out to be based in another country. However, it may be a matter for a UK force if:

- The people who created the material are in the UK.
- The material has been published from or downloaded onto computers in the UK.

- It might be evidence of offences committed in the UK.
- It might be evidence of crimes committed by UK citizens.

It has to be stressed that the police can only act against material that breaks the law. There is a great deal of material on the Internet that might cause offence but which is not technically illegal.

HOW CAN THE PUBLIC REPORT ILLEGAL MATERIAL?

In 1996, major Internet firms in the UK came together with the police to establish the Internet Watch Foundation (IWF) to act as a focus for removing illegal material from the Internet. It provides a hotline service to enable Internet users to report material they believe may be illegal. The IWF assess the material and then notify the Internet Service Provider (ISP) and the police.

The IWF is only able to deal with material that falls into the following three categories:

- Child pornography located anywhere in the world.
- Adult material that would breach the Obscene Publications Act, but only if the offending site or service is hosted or registered in the UK.
- Criminally racist material but only if the offending site or service is hosted or registered in the UK.

The procedure for members of the public to report offensive material is to contact the IWF at www.iwf.org.uk/hotline; the IWF will then make the decision as to what action needs to be taken.

Please do not contact the police directly. The IWF are qualified to judge the illegality of the material and will report the matter to the police if necessary.

The advice given is based on information supplied to Bedfordshire Police and current crime trends in the area. Bedfordshire Police Crime Reduction Officers can only give a view on what measures might reduce the risk of crime and there can be no guarantee that the measures will prevent crime. The advice is given without the intention of creating a contract and Bedfordshire Police has no legal responsibility for any advice given.

SECTION 7 : PROPERTY MARKING

WHY DO IT?

Property marking by itself cannot prevent a theft from happening but it can act as a deterrent to most thieves.

Not only that but in many cases if the property is not marked, the police cannot identify the rightful owner. Because of this, it makes it very difficult for the police to prove the item was stolen in the first place.

A frustrating situation, as you can imagine ... but there is a simple solution.

By using your postcode and house number, you increase your chances of recovered stolen property being returned to you.

ENGRAVING OR ETCHING

This method is suitable for many hard surfaces and can be done using an electric engraving tool or a hand engraver. It leaves a visible and permanent mark and is most suitable for items such as bikes, garden equipment and tools. These marking kits can be found in most DIY stores and cycle dealers.

ULTRAVIOLET MARKING

UV pens put an invisible mark on your property which can only be seen by using a UV lamp. Use UV marking when other methods could reduce the value and aesthetic of the object. Remember, however, that with some marker pens the ink can fade with age - especially when exposed to sunlight - and can be washed off so it will need to be renewed regularly.

STAMPING

Bedfordshire Police crime reduction officers also have a stamping kit for marking leather saddles. If you would like us to visit you and mark your tack, please contact us at the email address below with your contact details.

DNA TECHNOLOGY

There are products on the market now that use DNA technology. This means each kit issued has a unique identifying code embedded in it. Once you have bought a kit, you mark all your property and register your details and property marked with the supplier. These products are usually combined with UV substances so that the police can find it and connect the property with an offender. Such products include SmartWater, Alphadot and SelectaDNA - details of all these and similar products can be found on the Internet.

oakview sg18 8bb
#23 MK40 1HR
10 LU1 9PG
Smith MK44 2BD

SECTION 8 : RINGMASTER

WHAT IS RINGMASTER?

Ringmaster is a countywide database of local residents, businesses (urban and rural), schools and Neighbourhood Watch co-ordinators registered to receive messages.

The member chooses to receive either email or telephone messages.

Messages relate to:

- A single crime or incident
- A series of crimes or disorder
- A hot spot highlighted in the fortnightly tasking process
- Crime prevention advice

Members only get messages relating to their area and can possibly receive 1 or 2 messages a week.

Members are given the relevant Crime Reference, and a contact number to reply with information.

Members are given crime prevention advice to reduce further crimes in their local area.

WHAT SHOULD I DO IF I GET A MESSAGE?

Make a note of any details and let friends, neighbours and members of staff know about it.

WHO DO I CALL IF I HAVE INFORMATION?

You must decide how urgent information is.

Anything relating to a possible crime in process should be reported as a 999 call immediately.

Less urgent information can be passed to your local Control Centre or you can call CrimeStoppers in confidence on 0800 555 111.

**IF YOU HAVE ANY QUESTIONS ABOUT RINGMASTER, PLEASE CONTACT
sarah.stevens@bedfordshire.pnn.police.uk or call 01234 275288**

SECTION 9 : USEFUL CONTACTS

POLICE CONTACTS

Main Switchboard: 01234 841212

In Emergency or Crime In Progress: 999

Crime Reduction Office: North Beds: 01234 275273, Mid/South Beds: 01582 473159/78

Ringmaster - Bedfordshire: 01234 275288

Crimestoppers: 0800 555 111

WEBSITES

Home Office Crime Reduction - www.crimereduction.gov.uk/businesscrime

Information Commissioners Office - www.ico.gov.uk

National Counter Terrorism Security Office - www.nactso.gov.uk

National Plant and Equipment Register - www.ter-europe.org

National Security Inspectorate - www.nsi.org.uk

Secured By Design - www.securedbydesign.com

National Churchwatch - www.nationalchurchwatch.com

Action Against Business Crime (AABC) - www.businesscrime.org.uk

Association of British Insurers - www.abi.org.uk

British Chamber of Commerce - www.chamberonline.co.uk

British Standards (BSI) - www.bsi-global.com

Business Link - www.businesslink.gov.uk

Card Watch - www.cardwatch.org.uk

Chip and Pin - www.chipandpin.co.uk

Crime Concern - www.crimeconcern.org.uk

Fraud Advisory Panel - www.fraudadvisorypanel.org