BEDFORDSHIRE POLICE
fighting crime, protecting the public

Crime Prevention
ADVICE AND INFORMATION

LOOKING AFTER PERSONAL INFORMATION

If you saw a casually dressed man rummaging through a bin outside a house, would you suspect him of committing a crime or wish him luck in finding his house keys he CLAIMS to have dropped by accident?

Bin raiding is becoming increasingly common. Offenders collect personal and financial information from our discarded correspondence and use it to create an identity to obtain cash, credit and goods for themselves.

Not only does this cause large losses for the victims, but trying to put their affairs back in order proves to be a major headache. These crimes not only affect your financial dealings but can have an impact on such items as your driving licence and other legal documents.

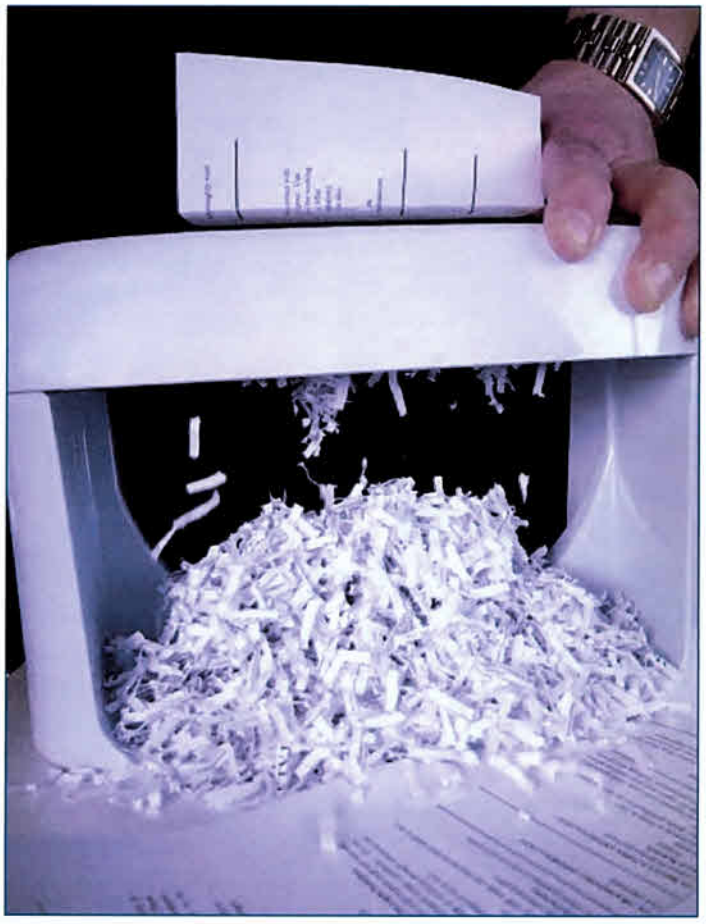
In 2010 an independent waste analysis company, with the support police, examined the contents of some 500 domestic bins in the city of Nottingham.

The findings will amaze you:

- 20% of bins contained a bank account number or sort code that could be related to the full name and address of an individual (this rose to 27% in more affluent areas).
- Only 8% of households throwing away paperwork containing credit card details attempted to destroy documents and only 1% succeeded.
- 8% of households threw away information providing at least 1 telephone number.
- 2% binned information providing a date of birth.
- One in six bins contained an intact utility bill.
- Around 25% of bins contained an official letter that could be used to corroborate identity.

Whilst the credit industry is working on ways to tackle identity theft, the first line of defence is changing your habits when it comes to your personal information. What can you do to prevent an offender from obtaining any document that contains personal or financial details or a signature? –

- **Tear up, shred or burn documents.**
- **Never put personal documents into a recycling bin.**
- **If you move house, redirect mail from Day One otherwise all kinds of bills and statements could fall into the wrong hands via your old address - especially if the new residents throw it away intact.**
- **Check your bank and credit card statements thoroughly and regularly to identify any unfamiliar transactions.**
- **Use different passwords for different accounts.**
- **Anyone who has been mugged or burgled might also fall victim to identity theft.**



BEDFORDSHIRE POLICE
fighting crime, protecting the public

Crime Prevention
ADVICE AND INFORMATION

AVOIDING 'PHISHING' SCAMS

Internet Banking is a safe way to manage your money. However, there are Internet fraudsters who will try to gain access to your accounts by emailing you and prompting you to disclose your online banking security details to them.

All British banks take Internet Banking security very seriously. They use the very latest industry-standard technology, plus multiple levels of security to safeguard your personal and transaction details so that you can bank online with confidence. However, each bank has a different policy so you need to check your own bank's guarantees and procedures if, in the unlikely event, you suffer from Internet fraud on your bank account.

Naturally, there is an expectation for you to exercise reasonable care to keep your security details secret at all times. The best way to do this is NEVER disclose any of your banking and personal details to anyone who calls on the phone or sends you an email, even if they claim to be from your bank or some other authority like the police.

How do fraudulent (Phishing) emails work?

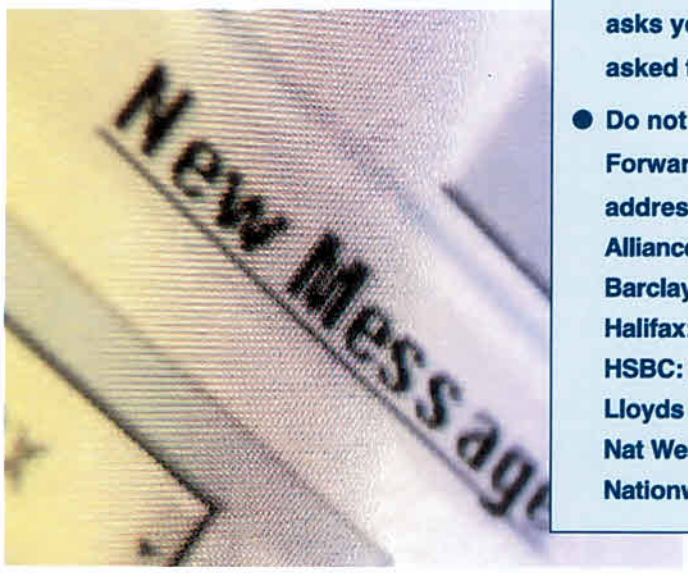
Typically, you will receive an email claiming to be from your bank, either requesting your security details (perhaps as part of an update or confirmation process) or asking you to follow a link to a site where you will be encouraged to provide a range of information such as your credit card number, personal identification number (PIN), passwords or personal information, such as mother's maiden name.

Clicking on the link takes you to a fake website, designed to look like your bank's website, but operated by the fraudster. Fraudulent emails and websites can be very convincing and fraudsters are continually inventing new approaches to try to get you to reveal your security details, so you need to be on your guard.

What do fraudulent emails look like?

To view copies of fraudulent emails that have been in circulation recently, visit **www.banksafeonline.org.uk.** You can also report phishing scams through this website.

Bank Safe Online is the UK banking industry's initiative to help online banking customers stay safe online and is run by APACS on behalf of its member banks.



What should you do to avoid being caught?

- **Monitor your accounts closely for any suspicious activity and contact your bank immediately.**
- **Firstly, your bank will never send you an email that directly asks you for, or links you to another page where you are asked to give your Internet Banking security details.**
- **Do not respond to any emails that request such information. Forward it to your bank – you will find a specific email address on their website. Some of the major banks are:**

Alliance & Leicester: suspiciousemails@alliance-leicester.co.uk
Barclays: internetsecurity@barclays.co.uk
Halifax: security@hbospIc.com / 0845 602 0000
HSBC: phishing@hsbc.com / 0845 600 2290
Lloyds TSB: emailscams@lloydstsb.co.uk / 0845 300 0116
Nat West: phishing@natwest.com / 0845 605 0789
Nationwide: phishing@nationwide.co.uk / 0845 730 2010

BEDFORDSHIRE POLICE
fighting crime, protecting the public

Crime Prevention
ADVICE AND INFORMATION

POSTAL SCAMS

Every day, people throughout the UK open their post to find they have unexpectedly 'won' a draw, lottery or other exciting prize. While much of this mail is genuine, some of it is a dishonest attempt to trap you into parting with your money.

How do you know it's a con

If you're asked to send money in order to claim your prize, then chances are it's a scam. Of course, like all con tricks, these postal scams are designed to catch you off-guard. Often the money is described as a 'management', 'administration' or 'handling' fee.

Or you may be asked to make4 a small purchase or call a premium rate number to claim your prize.

Either way, you'll be parting with money that you'll never see again – let alone your promised prize. So if you are at all unsure, ask yourself:

- **What am I being asked to pay for?**
- **Can I afford to lose the money?**
- **Does it look too good to be true?**

The warning signs to look out for . . .

- You are asked to send a fee to stake your claim
- The promotion is based overseas
- You are asked to send money abroad or to a PO Box number
- Prizes are shown in Euros or foreign currency
- You are asked for your credit card or bank account details
- You must persuade others to join a scheme in order to claim your prize
- It is an unsolicited letter, phone call or email
- You must respond at once to claim your prize
- You must purchase goods to claim your prize
- You must call a premium rate phone number
- If the wording says you 'may' have won a prize

What to do if you suspect a scam . . .

1) If you are not sure if it's a scam or not, put the mailing into the recycling bin (after removing any part containing your name and address).
2) If you think it's a scam and would like the Office of Fair Trading to investigate, send your suspect mailing to:
   The European Enforcement Team
   Office of Fair Trading, Fleetbank House
   2-6 Salisbury Square, London EC4Y 8JX
   Email: euroteam@oft.gsi.gov.uk
3) Inform your local Trading Standards Service office about the scam at:
   Bedford Borough Council
   Cauldwell Street
   Bedford MK42 9AP
   Central Bedfordshire Council
   Priory House, Monks Walk, Chicksands
   Shefford SG17 5TQ
   Luton Borough Council
   Clemitson House, 44-48 Gordon Street
   Luton LU1 2QP
4) Check to see if the company is a member of the Direct Marketing Association (DMA) – look for the DMA logo. Members must comply with a stringent code of practice.

Typical Scams – Get in the know or get caught out

- Letters telling you that you have won a prize which can only be claimed if you pay a 'processing fee'. The prize in question is usually far less than the fee.
- Letters asking you to 'invest' in a syndicate to increase your chances of winning a high-stake lottery overseas. This may result in unauthorised withdrawals from your credit card or bank account.
- Mailings from alleged clairvoyants (usually from Holland or Switzerland) inviting you to send money in exchange for good luck.
- Awards or other notifications of a large prize win. The small print requires you to send money for a piece of jewellery, which turns out to be virtually worthless.
- Official-looking invoices for payment to release a 'shipment' addressed to you.
- 'Cheques' made out to you requiring a 'document release fee' to receive the real cheque.
- Phone calls in which the caller identifies themself as an agent for a particular company, telling you that you have won a l;arge cash prize and asking you to send money to cover 'taxes'. This will result in inclusion on a 'sucker' list and yet more bogus mailings or calls.

REMEMBER – IF IT LOOKS TOO GOOD TO BE TRUE . . . THEN IT PROBABLY IS