

This factsheet will help you protect your business against frauds and scams, by making you aware of the most common types of each.

INTRODUCTION

Increasing numbers of frauds and illegal scams are directed at small companies and individuals. Greater use of the Internet is one reason for this increase, although it is not the only factor.

The National Hi-Tech Crime Unit (NHTCU) provides advice on a range of technology-based frauds. It recognises that improved technology has aided the development of new frauds whilst existing frauds have been adapted to exploit these improved technologies. Some common frauds include:

- Telemarketing frauds
- Advanced Fee frauds
- Lottery scams
- False billing
- Financial fraud
- Identity theft
- Phishing

These examples are not restricted to technology-based issues but they do rely on remote communication to further their aims. For up to date advice on this subject, you may wish to visit the DTI consumer guide web site at <http://www.consumerdirect.gov.uk>.

This factsheet is for any business wanting to increase its awareness about common frauds and scams. It covers many different kinds of frauds and scams, and how to react if you experience one of them.

TELEMARKETING FRAUDS

The global rise of telemarketing has produced a corresponding increase in telemarketing fraud. We are all vulnerable to illegal scams via

telemarketing (and by fax, e-mail and the post) but the following pointers highlight how you can protect yourself:

- If it seems too good to be true, it probably is. Think very carefully before committing yourself to any amazing 'deals'.
- There is no such thing as a 'guaranteed risk-free investment'.
- Beware of any unsolicited communication where you are asked to supply credit card or bank details.
- Beware of any unsolicited communication where you are asked to supply user names and passwords for services that you use such as online banking, online shopping, your Internet account, etc.
- If you receive a message advising that you have won a prize and should telephone a given number (often starting 900 or 0900), be careful! You will find that the telephone call is charged at premium rates and, in the unlikely event that there is actually a prize, it probably will not be anything worth having. In some cases you may even be asked to send a fee to cover postal costs.
- If you are offered something on a 'free trial' basis, always check deadlines for returning the items. If the scam involves obtaining credit card numbers illegally, you could be charged for goods even if you have no (knowingly) supplied any payment information.
- Think twice before giving information to unknown parties. For example, some fraudsters pretend to be charities (often using names that seem close to real organisations)

and ask for bank or credit card details. Other indications of possible fraud include:

- Being asked for your credit card details to verify that you really are a legitimate company
- Being pressured to allow the caller to send a courier around to take your payment
- Being told that you must act quickly or lose out on this one-time deal
- Being told of 'a little-known legal loophole' that will assist you in making a fortune
- Being told that you are one of just a few special people to receive this offer
- Being told that you have purchased the caller's services previously

What can you do?

One of the best ways to reduce the number of unsolicited telephone calls received (and so reduce the risk of fraud) is to register with the Telephone Preference Service (TPS). The TPS was formed in 1995 as a voluntary (self-regulatory) body to enable consumers to opt-out of receiving unsolicited sales and marketing calls.

You can subscribe to this scheme if you are an individual in other words, a private person, a sole trader or (except in Scotland) a partnership. For further information about the TPS or registering on the scheme, visit their web site at <http://www.tpsonline.org.uk/> Similar schemes exist for screening unsolicited post, e-mail and faxes. The Mail Preference Service (MPS) is a consumer service sponsored by The Direct Marketing Association (The DMA). The MPS was established to help consumers reduce the amount of non-profit or commercial mail they receive. You can find out more about the MPS at <http://www.dmaconsumers.org/offmailinglist.html> or visit the Direct Marketing Association web site at <http://www.dma.org.uk/> for further information.

ADVANCED FEE FRAUDS

AFFs often (but not exclusively) originate from parts of Africa. Nigeria is notorious for this type of scam, so much so that AFFs are often called '419 Schemes' after Section 4.1.9 of the Nigerian penal code. Common characteristics of an AFF scheme include:

- An individual or company receives a communication (e-mail, letter or fax) from a purported 'official' representing a foreign government agency. They will often claim to be a senior civil servant in one of the Nigerian Ministries, usually the Nigerian National Petroleum Corporation (NNPC).
- The fraudster offers to transfer millions of pounds into the victim's personal bank account, claiming that the funds have come from projects that have been over-invoiced or that they are excess funds from a previous political regime and cannot be accounted for.
- The pay-off is that the victim is offered a percentage of these funds for their trouble, often amounting to thousands or even millions of pounds.
- The perpetrator will induce a sense of urgency and stress the need for secrecy.
- Victims are often encouraged to travel to the source country to complete the transaction and are asked to pay various fees for the trip.
- Victims are nearly always asked to provide blank company letterhead, bank account information, telephone/fax numbers etc.
- Fraudsters will often send official-looking documents with seemingly authentic stamps, seals and logos all designed to enhance the authenticity of the deal.
- Sooner or later the victim will be asked to provide up-front or advance fees for various taxes, legal costs, transaction costs or bribes. Other variants of the AFF scheme include property ventures and offers of low-cost oil.

What can you do?

If you receive a message that you suspect is an AFF scheme or variant, do not respond. Even a tentative response will induce rapid, pressured communication, which will only prolong the correspondence. Some police forces ask that such communications be forwarded to them, so it is worth seeking advice from your local police force.

FINANCIAL FRAUD

If your business offers any form of online trading there are many ways you could be targeted by fraudsters. One of the simplest is the use of stolen credit cards to pay for goods or services. While card issuers carry much of the risk in such transactions, you are obliged to ensure that transactions are validated in accordance with your bank's contractual instructions. This is even more important when dealing with cardholder not present transactions, especially when the delivery address of the items purchased is different from that of the cardholder.

What can you do?

Your bank will issue its own instructions and guidelines for processing card transactions and these should be followed at all times.

Additionally, Card Watch is the UK banking industry's body that works with police, retailers and other organisations to fight plastic card fraud. It offers advice to retailers and similar organisations who accept card payments and has devised a Spot & Stop Card Fraud Pack to help prevent card fraud occurring at the sales desk or on the telephone. You can download this pack (free of charge) from:

http://www.cardwatch.org.uk/html/newer_spot_stop.html.

IDENTITY THEFT

Identity theft is when someone uses information about a person (or an organisation) to assume their identity. They will then try to obtain goods or services using that identity for example, jewellery, electronic items, bank loans and credit cards.

There are many ways in which an identity can be assumed. Some fraudsters read formal death notices in local newspapers and seek to assume the identity of someone who has recently died, while others scour rubbish bins behind offices and shops, looking for credit card slips.

There are also cases where fraudsters set up web sites to elicit information as part of a seemingly legitimate transaction a technique known as 'web spoofing'.

What can you do?

There are a number of things you can do to reduce personal and commercial exposure to the threat of identity theft. One of the most important steps is to ensure that your staff are aware of the risks. They are the people most likely to be contacted by potential fraudsters.

Some useful tips include:

- If someone telephones and requests personal information, be on your guard and ensure that the caller is genuine. If you are at all suspicious, ask for the caller's name and then use a directory to find their company's telephone number. When you call the company, ask for the person by name.
- If you have 'Caller ID' facilities (e.g. the 1471 telephone facility), check whether a caller has withheld their number. If yes, be wary.
- Be careful when establishing mail redirection services; there are people who use these facilities to claim personal and corporate identities.

- Destroy and carefully dispose of any financial or personal documents that are no longer required for example, bank correspondence, credit card slips and insurance forms.
- Check all of your credit card and bank statements. If you are unsure about a transaction, ask your bank to check it. If you have not received an expected statement, ask your bank why. If your bank advises that statements have been redirected to another address, make sure it understands the circumstances and takes appropriate action.
- Be careful when performing financial transactions online. Do as much as you can beforehand to ensure that the web site is genuine; check that the company has a secure site (e.g. a closed padlock) and look for information about the security protection the company has put in place. For specific consumer advice about safe shopping online, please visit the DTI's Consumer Direct website at <http://www.consumerdirect.gov.uk>
- Check your credit rating information periodically. Such information can tell you if there are other people using your corporate or personal ID. There are two main credit reference agencies in the United Kingdom Experian (<http://www.experian.com>) and Equifax (<http://www.equifax.com>). These agencies can advise you of your credit rating, usually for a small fee. Their web sites are also a good source of information about credit and identity fraud.

PHISHING

'Phishing' is the term used for the practice of sending false e-mail messages to a wide audience (using spamming lists) in the hope that some people will reply to them. Phishing e-mails are designed to look as if they come from a bank or similar organisation asking recipients to

confirm their account details (including account numbers and online banking security information). They usually give a plausible reason for requesting such details for example, to maintain an account.

An e-mail sent to Citibank customers in early January 2004 stated: "On January 10 Citibank had to block some accounts in our system connected with money laundering, credit card fraud, terrorism and check fraud activity. The information in regards to those accounts has been passed to our correspondent banks, local, federal and international authorities.

Due to our extensive database operations some accounts may have been changed. We are asking our customers to check their checking and savings accounts if they are active or if their current balance is correct." Links were given to false web sites, used to record information given for fraudulent purposes. The message was sent from an address that looked genuine and even asked customers to connect to a particular (false) web site if you suspect fraud.

Many 'phishing' e-mails do succeed (some suggest about 5%), with victims suffering identity theft and financial loss. One of the problems with such attacks is that the links provided in the e-mails go to false sites that look exactly the same as those they claim to be even the address looks the same.

The following UK banks have been hit by such attacks:

Barclays
NatWest
Lloyds TSB
Halifax
Bank of England

What can you do?

- Do not reply to such e-mails and never follow links provided. No bank would ever ask

customers to give such information in this way.

- A simple check would be to telephone your bank by a switchboard number or some other commonly known number and request more information. Do not use any telephone numbers given in the e-mail.
- If you are worried about information that you have already supplied, contact your bank and credit card company immediately.
- Passing details to the National Hi-Tech Crime Unit (<http://www.nhtcu.org/>) can help to reduce the impact of these scams.

GENERAL BUSINESS ADVICE

For more information on achieving best practice in your business contact your local Business Link advisor by visiting the website at <http://www.businesslink.gov.uk> or calling 0845 600 9 006.

Published by the Department of Trade and Industry. <http://www.dti.gov.uk> © Crown Copyright