



1. Bogus Credit Card Company Calls

Police are warning businesses to be vigilant following a spate of calls from a bogus credit card company. Several businesses have received calls from a woman claiming to be from the company. The woman requests details of their last three transactions and some businesses have fallen victim to the scam.

North Yorkshire Police are advising businesses to ensure their staff take full details from anybody claiming to be from a credit card company before divulging transaction information.

Anyone who receives a similar call should contact North Yorkshire Police on 01423 539334.

2. PayPal Customers Beware!

We have just received the following e-mail, ostensibly from the on-line credit card payment service "PayPal":

*From: "PayPal.com" <donotreply@paypal.com>
Sent: Wednesday, December 10, 2003 10:28 AM
Subject: YOUR PAYPAL.COM ACCOUNT EXPIRES*

Dear PayPal member,

PayPal would like to inform you about some important information regarding your PayPal account. This account, which is associated with the email address youremail@address.com will be expiring within five business days. We apologize for any inconvenience that this may cause, but this is occurring because all of our customers are required to update their account settings with their personal information.

We are taking these actions because we are implementing a new security policy on our website to insure everyone's absolute privacy. To avoid any interruption in PayPal services then you will need to run the application that we have sent with this email (see attachment) and follow the instructions. Please do not send your personal information through email, as it will not be as secure.

IMPORTANT! If you do not update your information with our secure application within the next five business days then we will be forced to deactivate your account and you will not be able to use your PayPal account any longer. It is strongly recommended that you take a few minutes out of your busy day and complete this now.

DO NOT REPLY TO THIS MESSAGE VIA EMAIL! This mail is sent by an automated message system and the reply will not be received.

Thank you for using PayPal.

Chamber comment: This message arrived with a virus infection, which was deleted by Norton Anti-Virus. Therefore, if you receive this message without such virus protection DO NOT OPEN THE ATTACHED FILE without making further enquiries. As we do not operate any PayPal Accounts it would appear to be a bogus message anyway.

As with any bank or credit card payment service, you are strongly advised not to give personal details on-line unless you are absolutely sure that the link is to the secure site operated by the correct organisation.

It is quite easy for criminals to fraudulently adopt a domain name like "PayPal.com" so that it looks genuine, but in fact it is not. If you have a PayPal account you would be advised to contact them directly.

The same problem occurred recently with WorldPay when criminals besieged the system with fraudulent messages attempting to gain personal data from account holders.

BUSINESS WATCH - Security Alert No 11 - page 2

3. Spam Law Clicks In

New rules to tackle 'spam' e-mails and give phone, fax and internet users more say over how their personal details are used come into force today. The rules, which apply the EU Directive on Privacy and Electronic Communication in the UK will mean that from today:

- Companies or individuals will not be able to send unsolicited commercial e-mails or text messages to individual subscribers unless the recipient has agreed in advance to receive them. There is an exception where businesses have established relationships with their customers.
- Corporate subscribers are exempt from this rule, which means that much business-to-business e-marketing is not affected. However all direct marketing e-mails, regardless of who they are sent to, will be required to include proper sender and contact details.
- Companies using tracking devices, such as 'cookies' on their websites will have to tell users they are doing so and provide an opportunity to reject them.
- Mobile network operators will be able to provide advertising and subscription services such as traffic information based on personal data, as long as they give subscribers information about this sort of data processing and obtain their consent.
- Subscribers will have legal rights about being listed in directories, and directory providers will have to give them full information and a reinforced chance to be 'ex-directory'.

Communications Minister Stephen Timms said: "The Office of the Information Commissioner, an independent authority that reports directly to parliament will enforce the regulations.

"Breach of enforcement orders issued by the Information Commissioner is a criminal offence liable to a fine of up to £5,000 in a magistrate's court, or an unlimited fine if the trial is before jury. Anyone who has suffered damages because the regulations have been breached has the right to sue the person responsible for compensation".

The Government is reviewing the enforcement and investigation powers available to the Information Commissioner.

4. Bin Raiding - think before you bin

Just as we have got used to being more careful in preventing credit card fraud, businesses and households across the UK are once again faced with a new wave of fraud that has reached us from the US called "bin raiding"! Although it is predominantly an urban phenomenon it is rapidly moving into rural areas, and involves individuals searching through people's refuse bins for personal information which can be used to commit fraud. A recent survey found that an average of 1 in 5 bins contain a bank account number and sort code that could be related to the full name and address of a household member. The survey also revealed that attempts by households to destroy personal information were very rare, with only 8% of households throwing away card numbers making any attempt to destroy the information, with only 1% being successful in rendering the information unreadable. Do you destroy your personal data?

Top Tips and advice to protect personal information:

- Never throw away whole receipts, bank statements, utility bills or any other documents that could be used by a fraudster to assume your identity.
- Always make sure personal information put into refuse bins is thoroughly destroyed using a shredder. You can also divide personal information into separate bags and dispose of it in different locations.
- Always check your bank statements against receipts and contact your card issuer or bank immediately if you find an unfamiliar transaction.
- Never give personal or financial information to cold callers.
- If you move premises ensure that your post is re-directed as new occupants may throw your mail in the bin instead of forwarding to your new address.