WEST YORKSHIRE POLICE

NOT WITH MY NAME

PROTECT YOUR PERSONAL INFORMATION

CITY OF LONDON POLICE
National Policing Lead For Fraud

ActionFraud
National Fraud & Cyber Crime Reporting Centre
actionfraud.police.uk

NOT WITH MY NAME

One of the simplest ways any of us can fall victim to a crime is by having our personal information taken from us online, over the phone or when out in the street and then used and abused by criminals.

More than one in four of us living in the UK has fallen victim to an identity crime, losing on average £1,200 each*. The knock-on effects can also be huge, causing massive personal distress and inconvenience and taking up to 200 hours of a persons' or businesses' time to fix. To add to the problem most people usually don't know their personal information has been compromised until it is too late, finding that:

- money has been withdrawn from their bank account without permission
- a fraudulent passport or driving licence has been created in their name
- loans, mortgages or mobile phone contracts have been set up in their name.

The good news is there are a number of simple steps you can take to safeguard your personal information. To reach as many people as possible with this important advice **West Yorkshire Police**, supported by the **City of London Police**, the **Metropolitan Police Service**, **Experian**, **Cifas**, **FFA UK**, **Get Safe Online** and **Cyberstreetwise**, is running a national campaign to raise awareness of this problem. Please take the time to read this leaflet and share it with family and friends.

*2013 National Fraud Authority Annual Fraud Indicator

TIP 1: BE CAREFUL WHO YOU GIVE YOUR PERSONAL INFORMATION TO...AND HOW

- Be very cautious about giving personal information – age, address, phone number etc – to people you don't know.
- In public places make sure nobody can hear your conversations or look over your shoulder when banking, shopping or making other confidential online transactions.
- Be careful with the amount of personal information you share online. Only make the minimum available (your name) on internet profiles such as Facebook and LinkedIn and don't post your address or date of birth.

TIP 2: MAKE IT AS DIFFICULT AS POSSIBLE TO CRACK YOUR PERSONAL PASSWORDS

Create strong passwords and use different ones for different accounts. For a secure password:

- use three words or more
- include a symbol and use upper and lower case letters and numbers.

Remember the more complex and unique to you your password is the harder it is to crack. Also don't keep a note of passwords where they could be lost or stolen – such as in your wallet or next to your personal device. For more information about staying safe online visit **www.cyberstreetwise.com** or **www.getsafeonline.org**.

TIP 3: ALWAYS DESTROY OR SECURELY STORE PERSONAL DOCUMENTS

- Check your bank and financial statements carefully and report anything suspicious to the bank or financial service provider concerned. When getting rid of personal documents always destroy them – rip up or shred.
- If you have a communal mailbox or one in a shared area, empty it frequently.
- If you move home set up a redirection with Royal Mail for at least a year and notify your bank, credit card companies and other organisations you deal with ASAP. Only 29% of British adults report redirecting their post when they move house.**

TIP 4: DON'T RESPOND TO UNSOLICITED PHONE CALLS OR EMAILS

- Fraudsters are increasingly targeting people over the telephone, posing as bank staff, police officers and other officials or companies to extract personal and financial information. Often the fraudster will claim there has been fraud on your account and that you need to take action.

Your bank or the police will never:

- phone you to ask for your 4-digit card PIN or your online banking password
- ask you to transfer money to a new account for fraud reasons
- send someone to your home to collect your cash, PIN, payment card or cheque book if you are a victim of fraud.

If you are given any of these instructions, you're being targeted by fraudsters. Hang up, **wait five minutes to clear the line**, or where possible use a different phone line, then call your bank or card issuer to report the fraud. For more information visit **www.financialfraudaction.org.uk**.

- If you receive unsolicited emails never reply with your full password, login details or account details. Don't click on any links as you could end up downloading a virus (malware).

Cifas National Survey, full details at **www.comres.co.uk

TIP 5: PROTECT YOUR PERSONAL DEVICES

- Protect all of your internet connected devices – computer, tablet, TV, mobile phone – by installing internet security software and ensuring that it is kept up-to-date.
- Make sure access to your devices is password protected.

ID CRIME IN ACTION

Sarah is a 31 year old professional who lives and works in Leeds. Earlier this year, Sarah and her neighbours noticed a stranger loitering near the lobby in their building trying to gain entrance to the communal post boxes.

A couple of days later, Sarah received a letter from a lender declining a loan application in her name for £8,000. The lender had declined the loan based on a small discrepancy in the information on the application. Shortly thereafter, Sarah received an application pack from a different lender for another loan for £10,000. This time, they were just waiting for completion of the application before processing the loan.

By contacting her bank and the other lenders concerned Sarah was able to close down both applications. Sarah also contacted a credit reference agency and had her details added to the Cifas protective register for 12 months.

ACT FAST IF YOU THINK YOU HAVE BEEN A VICTIM OF ID CRIME

- If you receive any mail that seems suspicious or implies you have an account with the sender when you don't, do not ignore it. It only takes 5 minutes to contact a credit reference agency over the phone to report your concerns.

- Get a copy of your credit report as it is one of the first places you can spot if someone is misusing your personal information – before you suffer financial loss. Review every entry on your credit report and if you see an account or even a credit search from a company that you do not recognise, notify the credit reference agency.

- Individuals or businesses who have fallen victim to a fraud facilitated by ID crime should report to Action Fraud on 0300 123 2040 or online at **www.actionfraud.police.uk**.

- If you have been a victim of ID crime you may also wish to take out Protective Registration with Cifas as an additional way to try to prevent fraud taking place in your name. Visit **www.cifas.org.uk/pr** for more details.

- If you have information about those committing identity crime please tell independent charity Crimestoppers anonymously on 0800 555 111 or at **www.crimestoppers-uk.org**.

PROTECT YOUR PERSONAL INFORMATION

age UK

cifas
Leaders in fraud prevention

CRIMESTOPPERS
0800 555 111
Call anonymously with information about crime

CYBERSTREETWISE.com

Experian™

FFA
Financial Fraud Action UK
Working together to prevent fraud

GET SAFE ONLINE .org

METROPOLITAN POLICE