This small booklet is available as both a PDF document for those who use computers but more importantly as a booklet for those who do not use computers or the internet.

Many of the scams detailed are in relation to those where the fraudster used either the telephone or cold calling at the victims front door. Unfortunately some of these scams reap larger rewards for the fraudster than many of the Internet frauds.

Obviously there are many other frauds not listed in this booklet such as those involving dodgy web-sites selling holidays, tickets for sports fixtures and concerts, fantastic deals on the latest mobile phones,auctions etc.

We can only re-iterate the following advice;

THERE IS NO SUCH THING AS " TOO GOOD TO BE TRUE" OR **AN OFFER OF SOMETHING FOR NOTHING**

Always check out who you are dealing with.

Peter Beck
Neighbourhood Watch Chairman
Rickinghall and Botesdale
01379 890495

RICKINGHALL & BOTESDALE

NEIGHBOURHOOD WATCH

SCAM ALERT

December 2014

STATISTICS

Every two minutes, someone in Britain loses their savings to a sophisicated new breed of conman

160,000

Computer Viruses sent by crooks every day to infect computers

26,995

Fake banks and building society websites reported last year

£450 million

Lost to fraud on bank cards in the UK

£ 37 Million

Lost to identity Fraud

£32 Million

Stolen from cash machines in *2013*

25-34%

of people who never ask a cold caller to prove their identity

USEFUL CONTACT NUMBERS

Action Fraud 0300 123 2040

Crimestoppers 0800 555 111

Action on Elder Abuse
0208 835 9280
0808 808 8141

Age UK 0800 169 6565

Alzheimers Society
0845300 0336

Financial Conduct Authority (FCA)
0800 111 6768

Mailing Preference Service (MPS)
0845 703 4599

Opt Out Services (mail addressed to occupier)
08457 950 950

Telephone Preference Service (TPS)
0845 070 0707

GOLDEN RULES

1. Be suspicious of all “Too good to be true” offers and deals. There are no Guaranteed get rich quick schemes.

2. Do not agree to offers or deals immediately. Insist on time to obtain independent/legal advice before making a decision.

3. Do not hand over money or sign anything until you have checked out the credentials of the company /individual

4. Never send money to someone you do not know or trust (whether in the UK or abroad)or use methods of payment that you are not comfortable with.

5. Never give banking or personal details to anyone you do not know or trust. This information is valuable Make sure you protect it.

6. Always log onto a website directly not by clicking on a link provided by an e.mail.

7. Do not rely solely on glowing testimonials; find solid independent evidence of a company’s success.

8. Always get independent/legal advice if an offer involves money,time or commitment.

9. Always ask for proof of identity from anyone knocking your door and request a contact land line telephone number.

10 If you spot a scam or have been scammed, report it to Action Fraud on 0300 123 2040 or online at actionfraud.org.uk. Contact the Police if the suspect is known or still in the area.

11. Do not be embarrassed to report a scam. Because the scammers are cunning and clever There is no shame in being deceived. By reporting it you will be making it more difficult to deceive others.

FRAUDS THAT MAY AFFECT YOU

BOILER ROOM

WINDOWS

S.O.S

IDENTITY

BANK CARDS

FAKE WEB-SITES

PENSION SCAMS

POLICE FINES

LOTTERY

BEQUESTS

WINDOWS

Most have received these unsolicited phone calls purporting to be from Microsoft Windows computer “department”.

The scam is basically an attempt (very often successful) to obtain your Bank details as shown on your debit card etc. The caller tell you that your Windows system is contaminated and requires repairing.

Cash is taking out of of your bank account and your details are then passed on to Criminal gangs for further theft of your money.

If you get such a call get as much detail as you can from the caller but;
DO NOT FOLLOW ANY INSTRUCTIONS THAT HE/SHE MAY GIVE YOU ABOUT THE KEYBOARD OF YOUR COMPUTER AND NEVER GIVE ANY BANKING DETAILS.

At the end of the call tell the caller you have not got a computer and your double glazing is satisfactory.

Pass any information gained to Action Fraud as it may help them build up their Intelligence base on these fraudsters.

SUFFOLK NEWS

At Ipswich Crown Court Mr.S. of Newmarket was sentenced to 4 years imprisonment for operating a fraudulent investment scheme where some £5 million was stolen from mainly East Anglian victims.

BOILER ROOM

Called Boiler Room as offices staffed by individuals who spend their time under pressure from their criminal bosses cold calling “victims” to sell shares in so called investment opportunities.

One can receive an unsolicited brochure giving a broad outline of some new fantastic opportunity to invest in a great profit making scheme.

LAND BANKING

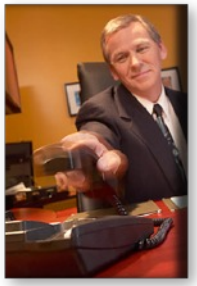
PHARMACEUTICAL

CARBON CREDITS

LAND PLOTS IN DIAMOND MINES

NEVER BUY INVESTMENTS FROM UN-REGULATED COMPANIES AND CHECK OUT THE ORGANISATION BY SPEAKING TO YOUR SOLICITOR OR FINANCIAL ADVISOR.

BANK CARDS



The telephone rings and the caller, allegedly from the bank claims that their may have been suspicious transactions in the use of a debit card in the victims name. The victim is advised to contact the bank on the telephone number on the reverse of the card.

The victim calls the bank and unknown to the individual the phone line is still connected to the caller who then goes through the procedure of security questions including all details of both the individual and the card.

The stolen details are then used to empty the targets bank account,and sold on to other crooks who clone the card

Sometimes a courier arrives at the victims house to collect the card and or to collect cash that the victim has been requested to withdraw from their account

BANKS WILL NEVER TELEPHONE YOU WITH SUCH MESSAGES. IF YOU RECEIVE SUCH A CALL HANG UP
DO NOT TRY TO RING YOUR BANK UNLESS YOU CAN USE A DIFFERENT PHONE.

S.O.S

One of the latest scams, usually by Russian computer hackers. Individuals who have e.mail/ Facebook accounts are targetted to obtain their friends contact e.mail addresses.

An e.mail from the fraudsters purporting to be from your friend is then sent to you.

The message claims that your friend has been robbed while on holiday and cannot leave wherever until a new passport is issued and they cannot leave the country until they pay hotel bills etc. The“Friend” then requests a transfer of funds to an exchange bureau.

DO NOT SEND ANYTHING UNLESS YOU HAVE SPOKEN TO YOUR FRIEND AND IF YOU CANNOT CONTACT THEM DO NOT , REPEAT, SEND ANYTHING.

LOTTERIES, PRIZE DRAWS SCAMS

Many have probably received unsolicited mail, leaflets etc giving the recepient the opportunity to play the lottery in Spain, Ireland and other foreign countries.
Also a letter may be received that you qualify for a free gift in respect of an unclaimed prize.

Subsequently your details are sent by the “lottery” organising company to the scamsters who then contact the victim saying that you have won a large cash prize. However to receive the money the victim is requested to send money to cover the expense of getting the prize funds released. Even after the victim sends the cash as requested further requests are made but the victim never receives the ficticious prize.

The unclaimed prize scam is similar as when the victim contacts the sender of the letter a payment is requested to cover postage etc. The prize that you may get is usually worthless rubbish.

Only purchase lottery tickets from established Lottery organisations at their Authorised outlets or regulated betting shops.

Do not answer unsolicited letters that advise you that you have won an unclaimed prize.

IDENTITY THEFT

There have been many cases where the identity of individuals has been stolen and used to obtain everything from mortgages credit cards and goods or services.

The problem is that many people do not ensure that their personal details are secure.

How many of us are on social media sites like Facebook where birthdays, family history,and other personal information is disclosed ?

How many of us leave correspondence on a window sill where anyone looking through the window can confirm your personal details?

How many of us throw away personal financial correspondence in the refuse bin?

How many of us answer unsolicited telephone calls or the door to door cold callers ?

Family and close friends will know your birthdays and Anniversaries. Why tell the rest of the world?

Never throw away personal mail , especially financial statements either shred them with a cross cutting shredder or burn them.

Check your bank/credit card statements to validate the transactions to ensure there are no duplicate or unknown transactions.

POLICE

The following scams are by fraudsters purporting to be Police officers using the normal understanding by the public that the Police would not act in such a way although the recent case where an officer was confiscating money from airline passengers leaving the UK from Gatwick Airport was not very helpful.

The following scams have taken place, some unfortunately in Suffolk.

ON THE SPOT FINES

Some of the adult web-sites are infected with a virus that automatically freezes the site and the computer's web browser.
A headed document ,usually with either the Lancashire or Metropolitan Police logos etc. appears on the computer screen stating that the victim has contravened a telecommunication act by viewing such adult material.
The victim is advised to pay a fine by money transfer agent. This cash can then be withdrawn at the agent by anyone who has the identication code which the fraudster will have been given by the victim on the false document.

The police have arrested some of these fraudsters but the advice is should you get such a message, switch off the power to your computer and re-start and delete the browser that you were using, close the computer down again then restart and re-install your deleted browser.

Advise Action Fraud of the incident and give all of the details you can.

The Police **NEVER ISSUE SUCH FINES ON THE INTERNET.**

.

COURIERS

The scamsters sometimes telephone the victim claiming to be Police Officers investigating a bank fraud and the fact that the victims card may have been the subject of fraud by a dishonest bank employee.

The victim is then requested to make a large cash withdrawal using the card and have the card and cash available for a courier to collect as the Police wish to introduce the cash back into the system so that the alleged dishonest employee can be identified.

Sometimes they request that the victim provides the card for collection by the police courier together with the pin-number. Very often the "courier" is an unwitting taxi driver who has been requested to pick up a package from so and so.

T**HE POLICE WOULD NEVER MAKE SUCH A TELEPHONE REQUEST AS OFFICERS WOULD VISIT POTENTIAL WITNESSES IN ANY CRIMINAL INVESTIGATION AND WOULD NOT ARRANGE ANY TRANSACTIONS OR USE OF THIRD PARTY COURIERS.**

BEQUESTS

There has been a number of these frauds where the victim is contacted by an unknown individual usually living in the Far East.

The fraudster claims that he knew a person living in his country who recently died. He has been trying to trace any relatives so that he can instruct solicitors to process the large sum of money in respect of the dead individuals estate. The “victim” is advised that as the only traceable relative it would be a good idea to let the fraudster help process the bequest through local solicitors.

To facilitate this “help” the fraudster needs funds to pay the solicitor. Official looking and headed letters are sent to the victim which appear to confirm the legacy.

The victim then starts sending money to the fraudster to process and obtain release of the bequest.

The promised money never arrives and some victims have lost thousands of pounds.

Should you get such a message or request pass the correspondence etc to your solicitor.

MIRACLE CURES

Too good to be true comes to mind.
There are hundreds of miracle cures available mainly on-line but also mailed to potential victim’s.home addresses. These cures are usually for Slimming but also go as far as claiming a cure for serious illnesses such as Cancer.

DO NOT BUY SUCH REMEDIES AND ONLY TAKE MEDICINES THAT HAVE BEEN APPROVED OR PRESCRIBED.

PENSIONS

Savers are being duped out of their pensions on their own doorsteps by motorcycle couriers who bully them into signing away their nest eggs.

The fraudsters are preying on the desperate who wish to get their hands on their retirement pots early.
They are conned into believing that the new Government Pension rules mean that they can obtain their cash immediately. After luring them by telephone a courier is sent to collect vital documents. On arrival the courier coerces the victim to sign release forms which allow the funds to be transferred to a rogue firm.

When someone does this before retirement age they get hit with a 40% arrangement fee by the crooks and subsequently a 55% tax charge. In other words they are left with £5,000 of a £100,000 Pension fund

These fraudsters are now moving onto the vulnerable who will be obtaining release of cash from their pension funds when they reach retirement age. Offering free advice they will then coerce and convince the victim to invest the cash into some dubious scheme.

AS STATED ELSEWHERE ONLY DEAL WITH REGULATED COMPANIES AND SEEK ADVICE FROM YOUR SOLICITOR OR FINANCIAL ADVISOR

CHARITIES

As a nation we all like to donate to charities to help those less fortunate than ourselves. However this area of obtaining money has also been used by the Fraudsters. Some charities have been used as a conduit and source of funds for criminal enterprises such as terrorist funding, drug trafficking and simply taking money for personal use by the collector.

Recently one such team of fraudsters manufactured charity wristbands naming a well known national charity.Their sellers in the high streets then sold the wristbands and kept the cash..

Recently it was also reported that another team were visiting public houses with official looking labelled charity collection boxes and obtaining cash for personal use.

A**LWAYS CHECK THAT THE INDIVIDUAL(S) SELLING IN A PUBLIC PLACE HAVE OFFICIAL IDENTIFICATION BADGES CONFIRMING THEIR IDENTITY ,THE REGISTERED CHARITY NAME AND NUMBER.**

Obviously it is always preferable to donate directly to the Charity of one's choice but as with anything involving payment check out the validity of who you are paying money to.

CAR PARKS

A common scam is where a smartly dressed individual approaches the victim in say the supermarket car park and offers luxury goods at a cheap cash price. Sometimes it's jewellery but can be sheepskin coats, suits,electrical goods etc. The claim usually is that they are either end of range or trade samples that he has been instructed to dispose of..

DO NOT BUY BECAUSE IF THEY ARE STOLEN YOU COULD BE RECEIVING STOLEN GOODS BUT USUALLY THEY ARE FAKE AND SECOND RATE ITEMS.

ACCIDENT CLAIMS

Over the past year a large number of fraudulent motor accident claims have been identified by both the Police and insurance companies resulting in a number of individuals being successfully prosecuted and imprisoned. However the scamsters are still out there so if you are involved in an accident take all of the details you can, time, date, weather situation, what happened , damage and personal Injury, insurance details of other parties involved, take photographs of the accident if you can (if you have a camera on your phone use that) names and addresses of other individuals including any witnesses.

Another scam is the text message on your phone telling you that as a result of your recent accident there are substantial funds awaiting you so please go to a computer website to complete the appropriate claim form. Of course that will require your bank account details which the scamster will then take money from , initially as arrangement fees and then a re-occurring charge. The"compensation is never given and the victim can be seriously out of pocket. Usually the scamster will make an excuse that there has been a problem with the claim and the other party or insurance company are now disputing the validity of it.

Only last week I received yet another of these messages, " £2917.44 is waiting in your name for the accident you had., To get this fill out "www.accidentinjuryclaim".so for us to transfer to your bank.". As I did not have an accident where I was injured and any such claim would have been dealt with by my insurance company - I immediately deleted.the message.

If you get such messages **DO NOT REPLY JUST DELETE THE MESSAGE.**
IF YOU GET A CALL ON YOUR PHONE LANDLINE JUST DO NOT ANSWER BUT HANG UP.

JOB OFFERS

Many of us like the idea of earning extra money. One such job offer frequently advertised is a work from home position where one acts as a commission agent purely receiving money transfers into your bank account and then transferring it onwards to another account, the commission being a percentage of the money transfer.

Beware as these jobs are usually a cover for money laundering and your bank account is being used to help conceal the actual origins of the (proceeds of crime) **dirty money.** If a criminal investigation is undertaken and the criminals caught,arrested and charged then, If you are acting as a conduit for this **dirty money** through your bank accounts , you could also be arrested and convicted. If the money laundering involves a foreign jurisdiction one could also be extradited to that country and face prosecution in the criminal courts of that country.
The U.S.A are certainly very draconian in acting against anyone In the world who breaks their laws especially when U.S. Currency is involved

DO NOT ALLOW ANYONE WHO YOU DO NOT KNOW USE YOUR BANK ACCOUNTS OR EVEN SET UP A SEPERATE BANK ACCOUNT FOR SUCH TRANSACTIONS.

We all moan about the hassle of proving who you are when dealing with the banks. The reason is the basic principle to stop money laundering which is;

"KNOW YOUR CLIENT"

In fact that is a message that we all should follow;

KNOW WHO YOU ARE DEALING WITH OTHERWISE DO NOT DEAL WITH THEM

ATM - CASH MACHINES

SEVEN SIMPLE RULES

1. NEVER share your PIN with anyone the only time you should use your PIN is at a cash machine or when you use a chip and PIN machine in a retail establshment.

2. If there is any sign of something unusual about the cash machine or there are signs of tampering do not use it and report it to the bank as soon as possible.

3. Cover your PIN. Stand close to the machine and always use your free hand to cover the keypad as you enter your PIN to prevent any prying eyes or hidden cameras seeing it.

4. Do not get distracted. Be particularly cautious if "well meaning strangers" try to distract you or offer to help you. More importantly discreetly put your money and card away before leaving the cash machine.

5. If your card does not get returned to you once it has been put in the machine immediately contact your card issuer to cancel the card whilst you are still at or near the machine. Ensure that you have your issuer's 24 hour contact number In your mobile phone or in your wallet and purse.

6. NEVER write down your PIN number on paper or on your Mobile phone as if your wallet/purse or phone is stolen with Your card you could have a major problem.

7. The bank, Police will never ask to collect your card and your PIN