OUT OF THE BLUE OR TOO GOOD TO BE TRUE

THINK FRAUD · THINK FRAUD · THINK FRAUD

STOP / CHALLENGE / CHECK

HEDDLU
GOGLEDD CYMRU
NORTH WALES
POLICE

Introduction

Welcome to the North Wales Police fraud prevention booklet. In it you will learn about the current scams we are seeing in the area, as well as practical advice on how you can best protect yourself from criminals intent on getting their hands on your money.

In 2021 North Wales Police created a new Economic Crime Unit, bringing together financial investigators, financial safeguarding officers, specialist fraud investigators and cybercrime officers, to reduce the harm caused to our residents by fraudsters.

Over £10 million is lost to fraud every year in North Wales alone, and with a significant number of criminals operating from outside the UK, investigation and recovery of lost funds can prove challenging. As such, we believe that preventing fraud and raising awareness is the key to protecting everyone in our community. If you can recognise fraud when it happens, you can stop yourself becoming a victim.

Fraudsters are constantly formulating new ways to deceive their victims and will use modern technology to hide their identity or convince you they are genuine. This means that spotting a scam isn't always easy but generally, if something sounds too good to be true, or if the contact you receive is unexpected, then it is likely to be fraudulent.

We hope you find the information in this booklet useful, and that it increases your awareness of fraud so that you can avoid any financial loss. We would also ask that you share this information with your friends and family so that everyone in North Wales becomes fraud aware.

Content

Message from the Chief Constable

Chief Constable
Amanda Blakeman

As Chief Constable of North Wales Police my aim is to make North Wales the safest place to live, work and visit. This booklet designed and prepared by officers from the Economic Crime Unit gives information and advice to prevent you, your friends and family becoming victims of fraud. I would ask that you consider the information carefully and take action to look after your finances and your assets. We need to work together to make it as difficult as possible for fraudsters to commit these crimes. Personal awareness around the type of crimes committed and how they occur is the first step to stopping fraud from happening and this booklet provides this in respect of the crimes we see in North Wales annually.

Message from the PCC

Andy Dunbobbin
North Wales Police and
Crime Commissioner

As your Police and Crime Commissioner I want to help the people of North Wales to become more resilient and resistant to the threats posed by fraud.

Fraud is gaining a dishonest advantage, often financial, over another person and is now the most commonly experienced crime in Wales.

The impact of fraud can be devastating, ranging from unaffordable personal losses suffered by vulnerable victims to impacting on the ability of organisations to stay in business.

We work with partners from across the public, private and third sectors to pursue serious and organised fraudsters and make individuals and businesses safer from fraud and other economic crimes. We invite you to use the information and advice in this booklet to protect yourself and those you care for.

Telephone scams

The telephone is the most common method fraudsters use to make contact with their victims. Criminals may claim to be from a wide variety of organisations such as a bank, a government agency, a utility company, a computer software provider or even the police, and will attempt to manipulate you into acting on their instructions.

They may ask you to provide your personal information, including your bank details, to receive a refund or pay for something. This information can be collected by the criminals and used to steal your identity, opening accounts or accessing existing accounts in your name. This is also known as ‘vishing’.

They might request remote access to your computer to fix a fault or try to persuade you to transfer money from your account into another safer account. Criminals may also offer to send a courier to your home to collect cash or other valuables, or ask you to post your bank cards or cash in the mail. All of these requests are likely to be fraudulent.

The number that appears on your caller ID may look familiar or match the number on the back of your bank card, but this can be faked and even if the caller already has some of your personal information, this does not guarantee they are a genuine caller.

Scammers can keep a telephone line open even if you have ended the call. The line can be kept open for up to ten minutes, so if you need to verify a suspicious call, we recommend that you use a different line, a mobile phone or ask a friend or family member to check the validity of the call using their phone.

A common tactic used by criminals is to ask for gift vouchers as payment. This kind of request will always be an indicator of fraud as no legitimate payment can ever be made using vouchers.

Although spotting a fraudulent call can be tricky, be aware of any request that is unexpected or unusual and trust your instinct. Fraudsters will often want you to act quickly, putting you under pressure to act without thinking.

REMEMBER...

- A legitimate organisation won't mind if you want to take time to confirm the call is genuine.
- No company will ever ask you to download an app to gain remote access to your computer.
- Do not give out any personal details, bank information or one-time passcodes to ANYONE over the telephone.

PROTECT...

- Where possible, don't answer the phone to unrecognised numbers and let your answering machine take a message.
- Register your landline and mobile number with the free Telephone Preference Service to opt out of unsolicited sales and marketing calls.
- Contact your telephone provider to ask what call protection service they offer.
- Purchase a call blocker that can restrict the calls being made to your landline telephone.
- Report scam telephone numbers to 7726.

STOP / CHALLENGE / CHECK

STOP – be suspicious of any unexpected call and take your time.

CHALLENGE – don't be afraid to say 'no'.

CHECK – verify the call is genuine using contact details from an independent source.

Shopping and selling online

Criminals regularly target victims who shop online, both as buyers and as sellers, and use a wide range of tactics to target their victims.

This fraud type can include fake or cloned websites that are designed to mimic a legitimate company. Fraudsters may also set up companies offering inferior or counterfeit goods for sale online at high prices which may include fake reviews or unrealistic claims.

Auction sites are regularly misused by fraudsters in a number of ways, so we always recommend that you check the site's payment policies before making any purchase. You should be wary of any seller requesting a large deposit or even payment in full direct into their bank account, rather than using PayPal or other similar services. Criminals who commit this type of fraud will then cease all contact once payment is made and you will not receive any goods. If you make a payment against the advice of the auction site, the purchase will not be protected, and you are unlikely to be refunded.

PayPal's 'Friends and Family' option allows users to send money to others without incurring a fee, but it is designed to be used by people who know each other. If a seller you don't know asks you to pay using this feature be aware that there will be no protection if the seller turns out to be a criminal.

Criminals may also approach sellers who are offering high value items for sale, such as mobile phones, tablets or laptops which they then offer to purchase. Once the price has been agreed the fraudster sends a fake email, that appears to have been sent by PayPal, stating that payment has been made and that the item can be posted. Victims of this crime only realise the PayPal email was fraudulent once the item has been sent but no funds have entered their PayPal account.

Fraudsters offering to buy goods could also come to your home address to collect items you are selling. If you accept cash as a method of payment, be aware of counterfeit currency and check you have been given the correct amount of money before handing over your property. In some cases, criminals have been known to insist on paying by bank transfer. They then show a fake banking app as proof that payment has been made. Remember to check that funds have entered your bank account before allowing the buyer to leave with the goods.

REMEMBER...

- Be wary of offers that look too good to be true.
- If you are selling an item, double check that you have received full payment before sending or handing over your possessions.
- Just because something looks genuine doesn't mean it is.

PROTECT...

- Don't make payment direct into a seller's bank account.
- Use the payment method recommended by the auction site you are using, such as PayPal.
- Avoid using PayPal's 'Friends and Family' option to pay people you don't know.
- Don't accept an email as proof of payment - if you are expecting a payment, check your account by logging in directly.

STOP / CHALLENGE / CHECK

STOP – take your time to research online sellers and websites.

CHALLENGE – don't be rushed into making a sale or a purchase.

CHECK – make sure you have received payment before posting or handing over an item.

Text, WhatsApp and email scams

More and more of our communication now takes place online and fraudsters have found several ways to exploit this.

Criminals can contact their victims by sending official looking emails or text messages that appear to come from legitimate companies and organisations. These are designed to lure you in by promoting discounts or special offers, requesting you update your account details or advising there is a problem with your bills or banking that you need to address.

Often, within the body of a fraudulent email or message, there is a link for you to click which may take you to a web page. These fake web pages, also known as cloned sites, are designed to replicate the official website you may be familiar with. When on the fraudulent web page, you will be asked to supply your personal information, and you may possibly be asked to enter your password. This information is harvested by the scammers and will enable the criminals to access your genuine account or commit identity theft.

Clicking on links provided in fraudulent emails may also result in a computer virus or malware being downloaded onto your device so it is important to be wary, especially if the email or text message is unexpected.

Sextortion is a common scam seen on email accounts. This is where criminals send an email claiming they have hacked into your device and obtained your personal information, such as your usernames and passwords, or taken screen shots of websites you have visited. Some will even claim they have evidence you have been viewing pornographic material and request payment to prevent this information being released. Often the email will appear to have been sent from your own email address, or may contain a password you have previously used, to convince you that your device has been hacked into and your information compromised. In most cases however, these emails are sent by opportunists and, if ignored, will come to nothing. If you receive an email like this, you should not respond and you should never pay money when demands like this are made.

Email and text message scams are more difficult to spot when the message appears to have come from a friend, colleague or another person known to you. You may be more inclined to believe the content of the email or message if it has been sent by someone you trust, but you should be aware that criminals can use this to their advantage. If you receive a request for money to be sent, vouchers to be purchased or suggestions you are eligible for a grant, benefit or prize money, it may be that the other person's messaging account has been compromised and the request has been made by a fraudster. You should check with the sender that the request is genuine before taking any action.

WhatsApp can also be used by criminals to trick you into parting with your money. A common fraud involves scammers sending a message, claiming to be a family member with a new mobile number. The criminals, pretending to be a family member, then message to say that because their old phone has been lost or damaged, they are unable to access their bank accounts and need your help to pay an urgent bill. You should always be cautious when someone contacts you asking for money, even if the request seems genuine.

REMEMBER...

- Criminals can make any electronic communication appear legitimate by using logos and formats you recognise.
- A genuine company will never ask you to confirm your personal information, PIN, or passwords.
- Fraudsters may impersonate a friend or family member to extract money or information from you.

PROTECT...

- Don't give out personal information to anyone, even if the communication looks genuine.
- Don't click on links contained within emails or text messages unless you are certain it is legitimate.
- Double check any communication is genuine, especially if you have received a request for money, vouchers or to provide personal information.
- You can forward scam text messages to 7726.
- Forward scam emails to report@phishing.gov.uk

STOP / CHALLENGE / CHECK

STOP – take your time and think about each email, text or WhatsApp message you receive.

CHALLENGE – report any message you think might be fake to 7726 or report@phishing.gov.uk

CHECK – take steps to check the communication is genuine before you act.

Investment fraud

The idea of making money through investment appeals to many people and investments can be a successful way of earning. But it can also be risky, with fraudsters preying on investors and causing people to lose their life savings.

Criminals have been known to offer investments in a wide range of products including carbon credits, wine, metals, diamonds, foreign exchange (also known as Forex or FX markets) and crypto currency.

Fraudsters will often target their fake investments at the elderly or those newly retired who have access to their pension pots, promoting their investments using glossy brochures and professional looking websites. They may also include fictitious celebrity endorsements or fabricated testimonials to make their venture seem more appealing. The company may even have been registered with Companies House, using an up-market address, but the address is likely to be a post office box or a rented virtual office space. Criminals can also 'clone' well established investment companies to dupe their victims.

Often, those targeted receive telephone calls and emails that appear out of the blue. Sometimes victims are identified after replying to a pop up on a computer or an advert containing a link which then requires you to supply some of your personal details to arrange a call back from the fake investment company.

Criminals posing as investment managers often downplay the risks involved, making promises of swift, high returns. They will urge you to act immediately to avoid missing out on a the time-limited offer. This sale pitch is designed to make you act without thinking clearly or making the necessary checks about the company. You may be kept on the phone for hours at a time, all the while being persuaded to part with money.

In order to prove the legitimacy of the investment you may be asked to invest a small amount in the beginning which you will be told has increased in value significantly within a short space of time. In some cases, victims are given some of their original investment back as a return, but this tactic is used solely to build confidence in the fake investment, encouraging further investment of much larger sums.

Once a large investment is made it becomes impossible to extract any money from the investment. Criminals will ask for more and more money for further investment, fees and tax payments to enable a withdrawal, or they may cease contact altogether.

If you have already lost money to an investment fraud it is possible that you will be contacted again by a company claiming they can recover your lost funds. This fraudster may be linked to the initial group of criminals, so may appear to know a lot about your situation. You will eventually be asked to pay upfront for the money to be returned to you, but you will never get your money back once you have paid for their services.

REMEMBER...

- Legitimate companies will not contact you out of the blue to offer lucrative investment opportunities.
- Criminals will use various tactics to convince you their offer is genuine.
- If an offer seems too good to be true, it usually is, and even genuine investments carry risk.

PROTECT...

- Don't reply to emails and reject any cold call offering investment opportunities.
- Don't supply your personal information to people you don't know.
- Conduct thorough checks on any company you plan to invest with and check the Financial Conduct Authority Warning List online.
- Take advice from an authorised Independent Financial Advisor who is registered with the Financial Conduct Authority.
- Beware of companies based overseas as they are unlikely to be regulated and may not be authorised to operate in the UK.

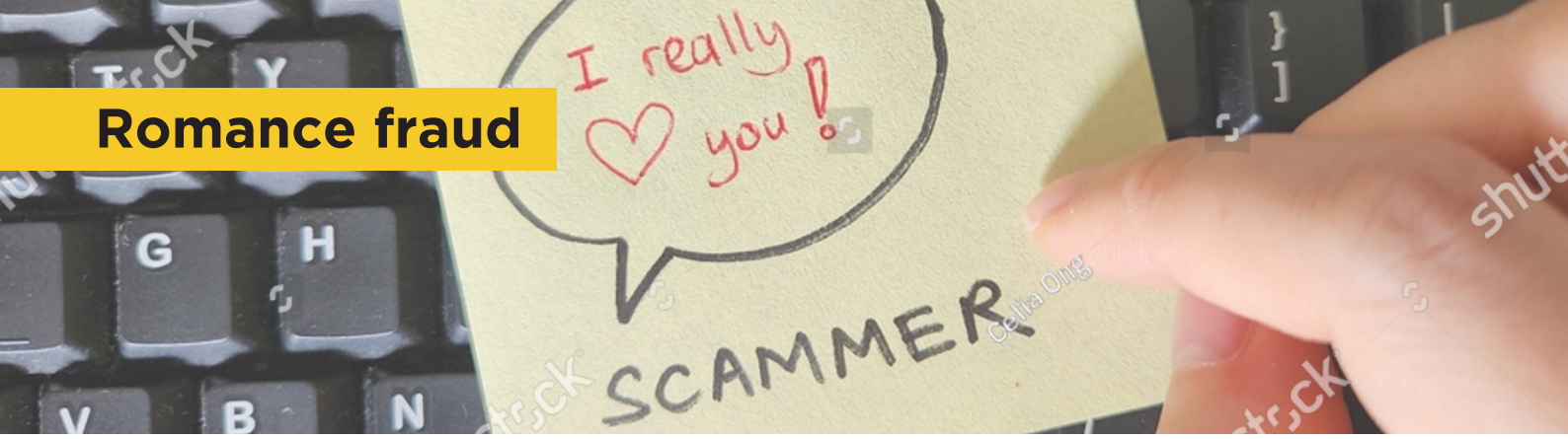
STOP / CHALLENGE / CHECK

STOP – don't be rushed into making a decision about any investment.

CHALLENGE – don't engage with cold callers and report any suspicious emails to report@phishing.gov.uk

CHECK – ensure the company you are dealing with is authorised to operate in the UK and is regulated by the Financial Conduct Authority.

Romance fraud



Dating websites and social media sites are one of the most popular ways to meet new people but unfortunately, amongst the genuine profiles, there are fake profiles created by criminals whose intention is to manipulate you, take advantage of you and trick you into handing over your money. These fake profiles are designed to appear attractive and use images stolen from the internet to disguise the scammers' true identity.

There are several warning signs that point to an online acquaintance being a fraudster, one of which is the current situation they claim to be in. Typically, a criminal will say they are abroad in a remote country, working on an oil rig, in the army or are in another line of work that makes it difficult for you to verify if what they are telling you is the truth.

Another indicator of fraud is the speed at which the relationship develops. They will be very flattering, attentive and speak of your relationship being romantic within a short period. They will message frequently, building trust and emotional attachment and may even discuss a personal problem they have to gain your sympathy.

They may also suggest moving your conversation away from the official dating site or social media site to a more secure messaging service. They will say that this is so that you can converse in private away from anyone prying into your conversation, but in reality it is so that they can continue contact with you even if their dating profile is removed from the dating site and to isolate you from friends or family who may show a concern about the relationship.

Romance fraudsters will often talk about a future together with you, appearing eager to meet in person, but they will provide a range of excuses as to why a meeting can't take place, such as being arrested, having no money for a flight, or being involved in a car accident preventing them from travelling to see you. Quite often there will be one problem after another that keeps them from meeting you in person. They may also be reluctant to take part in a video call or voice call and insist on the conversation taking place by message only. This is because they are not who they say they are, and a video or voice call would expose them and their lies.

Eventually the fraudster will begin asking for money to help with a fabricated issue they have and will manipulate you into feeling guilty if you do not comply with their request, using emotional blackmail and a sense of urgency. They may say they need money for a sick relative, bail money following an arrest, money to release an inheritance or money to get them out of the armed forces so that they can be with you. Sometimes a third party will be introduced, such as a fake solicitor, to make the lies seem more believable but this person is also part of the scam.

You may be asked to accept money into your bank account from another source to send to the suspect. In these circumstances the money is likely to have come from another victim of fraud and you are being used to launder money, which is a criminal offence.

REMEMBER...

- Stay on the dating site and avoid isolating yourself with the fraudster.
- Watch out for a relationship moving quickly, with early declarations of love before you have even met in person.
- Not everything someone tells you about themselves online is true – don't take everything on face value.

PROTECT...

- Reverse image search the profile pictures or images you have been sent to see if they have been stolen from the internet or manipulated.
- Never send money to a person you have met online, no matter what they tell you or even if they promise to pay you back.
- Never accept money into your own bank account from another on behalf of someone else.
- Be aware of the information you are giving out about yourself and talk to your friends and family about your relationship.
- Report any suspicions you have to the dating or social media site.

STOP / CHALLENGE / CHECK

STOP – never send money to someone you have met online, no matter the reason they give you.

CHALLENGE – don't be pressured into moving away from an official dating site.

CHECK – think carefully about what you are being told and if there is any way to verify the information you have.

Cybercrime

Many people now have access to the internet and are online daily whether to shop, carry out online banking or to stay in touch with friends and family. Although the internet is convenient and more accessible than ever, there are risks associated with its use.

Hacking is the term used when a criminal accesses a computer system or network, usually to gain unauthorised access to personal data. Hacking is often a precursor to fraud taking place.

Criminals will use a variety of techniques to access the data they want. Fraudsters can use social engineering to manipulate you into handing over passwords voluntarily. You may receive a fraudulent email, text message or visit a fake website with a link, where you will be asked to supply your personal information or enter your password. This information is harvested by the criminals who use it to commit fraud or identity theft.

Hackers may also use a 'trial and error' method where they use a computer program to try to guess your password which they can then use to access your account. If you use the same password repeatedly then the criminals can commit identity theft and take over all your online accounts.

Alternatively, they may infect your device with malware, which is malicious software designed to infiltrate your device that has been hidden in a link, an email attachment or a download. The malware then records all the information on your device, and monitors which websites you visit whilst recording the passwords you type. It can also block access to your files, bombard your desktop with adverts or render the device inoperable. You may then be asked to pay a 'ransom' to the hackers in order for them to release your data back to you.

Although this may seem daunting, there are some simple steps you can take to protect yourself.

PROTECT...

- Choose your passwords carefully and keep them secret. It is recommended that you use three random words and include lower-case and upper-case letters as well as numbers and special characters to make it difficult to guess.
- Use a different password for each account. You can use a password manager to help keep track of them.
- Ensure you have internet security software on all your devices, including smartphones and tablets. You need to make sure that this is kept up to date and is always turned on.
- Download and update your operating system and app updates when prompted as these contain security updates.
- Don't assume Wi-fi hotspots are secure. Wi-fi offered in places like cafes, hotels and restaurants should never be used to carry out confidential activity online.
- Never disclose passwords, PINs or personal details online, on social media or within an email.
- Beware of fake emails, messages or phone calls as they may not be legitimate.
- Don't click on links contained within emails, messages, posts or tweets and don't open any attachments if they are unexpected and not from a source you know and trust.
- Use Two Factor Authentication (2FA) where possible.
- Use PINs or passwords to lock your devices when not in use.
- Ensure your privacy settings on social media accounts are correctly set so that only people you know can see them.

STOP / CHALLENGE / CHECK

STOP – take your time and think twice before clicking links or opening attachments.

CHALLENGE – check your credit score and bank statements regularly to spot any irregularities.

CHECK – if you receive any contact that is unusual or unexpected, contact the individual or organisation to make sure it is genuine.

Notes

Use these pages to note down any important information such as suspicious phone numbers, names, times and dates or report reference numbers you may need later.

How to report

Should the worst happen, and you fall victim to fraud, here are the steps to take and who you should contact.

Protect your accounts

If you have given out your bank details, even if no money is missing, contact your bank **immediately**. They can then act to protect your account and replace your bank cards to prevent fraudulent transactions.

If you have lost money, you may be entitled to a refund from your bank under the Contingency Reimbursement Model. For details visit **www.financial-ombudsman.org.uk** to see if you can make a claim.

Write your bank's contact details here in case you need them in an emergency

.....

Report a crime

If the fraud is in progress and there are suspects present, report direct to **North Wales Police on 101** or if it is an emergency dial **999**.

Otherwise, you should report the matter to **Action Fraud** on **0300 123 2040** or at **www.actionfraud.police.uk**. Action Fraud are the national reporting centre for fraud across England and Wales.

Check your credit

If your personal information has been disclosed, it is recommended that you check your credit score. This will show you if your details have been used to open credit accounts in your name. It is good practice to check this periodically even if you haven't been the victim of fraud.

If you are still concerned about identity theft you can join the **CIFAS Protective Register**. For a small fee you will be made aware if a credit account is opened in your name as additional security checks will be made directly with you. Find out more information at **www.cifas.org.uk/pr**.

Report suspicious calls, text messages and emails

You can report fraudulent phone calls, text messages and emails directly, even if you haven't lost any money. This information is used by the National Cyber Security Centre and Ofcom to protect others.

To report a scam call text the word 'Call' followed by the suspect number to **7726**, which spells out SPAM on your keypad.

To report a scam text forward the message to **7726**. More information can be found at **www.ofcom.org.uk**.

You can report a suspicious email by forwarding the email to **report@phishing.gov.uk**. More information can be found at **www.ncsc.gov.uk**.

Useful contacts

Action Fraud
0300 123 2040 and www.actionfraud.police.uk

North Wales Police
101 or 999 in an emergency and www.northwales.police.uk

Friends Against Scams
www.friendsagainstscams.org.uk

Citizens Advice Bureau
0800 702 2020 and www.citizensadvice.org.uk/wales

Get Safe Online
www.getsafeonline.org

Age UK
0800 678 1602 and www.ageuk.org.uk

Victim Support
0808 1689 111 and www.victimsupport.org.uk

Financial Conduct Authority
www.fca.org.uk

Financial Ombudsman
www.financial-ombudsman.org.uk

Take Five
www.takefive-stopfraud.org.uk

Samaritans
116 123 and www.samaritans.org/wales

National Cyber Security Centre
www.ncsc.gov.uk

Rhybudd Cymunedol Gogledd Cymru
North Wales Community Alert

86253.

Sign up today to North Wales Community Alert

North Wales Community Alert is a **free** community messaging service brought to you by North Wales Police and partners.

By registering you can receive up to date information on crime, missing and wanted appeals, crime prevention advice, engagement events and general policing activity in your local area.

You can **reply** to messages and provide feedback to your local neighbourhood police team on the issues that matter most to you, helping us to work together to make North Wales the safest place in the UK.

Registration is complete free, quick and simple.

Visit **www.northwalescommunityalert.co.uk** and sign-up for free today.

SWYDDFA **COMISIYNYDD HEDDLU A THROSEDD** GOGLEDD CYMRU
OFFICE OF THE **POLICE & CRIME COMMISSIONER** NORTH WALES

HEDDLU GOGLEDD CYMRU
NORTH WALES POLICE

making North Wales the **safest** place in the UK