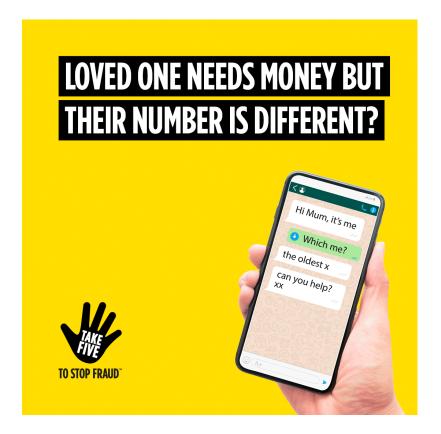
WhatsApp Scam Messages 24.05.2023 Gloucestershire Constabulary are working in partnership with your GP Surgery to share Fraud Prevention Advice on a regular basis.

The National Fraud Intelligence Bureau (NFIB) is warning the public about the continued increase in reports about scams where victims are targeted on WhatsApp by criminals pretending to be someone they know – typically their children.

Criminals will usually begin the conversation with "Hello Mum" or "Hello Dad" and will say that they are texting from a new mobile number as their phone was lost or damaged. They will then ask for money to purchase a new one, or claim that they need money urgently to pay a bill.



The criminal will provide bank details for the payment to be made to, with some criminals coming back with further demands for money.

Between 3rd February 2022 and 21st June 2022, there have been a total of 1235 reports made to Action Fraud linked to this scam, with total reported losses exceeding £1.5 million.

What you need to remember:

- 1. **STOP. THINK. CALL.** If a family member or friend makes an unusual request on WhatsApp, always call the person to confirm their identity
- 2. You can report spam messages or block a sender within WhatsApp. Press and hold on the message bubble, select 'Report' and then follow the instructions

3. Never share your account's activation code (that's the 6 digit code you receive via SMS)

Under-reporting is a real issue with these sorts of crimes as victims wrongly believe they would be wasting our time, there's nothing that can be done or they feel embarrassed by what has happened.

We urge anyone who may have experienced this situation to report it to Action Fraud on 0300 123 2040 or at www.actionfraud.police.uk

Online Shopping 24.05.2023

Online shopping fraud is the number one reported fraud type at the moment across the UK, and we are seeing increased reports within Gloucestershire.

We have seen reports of small items being purchased to holidays, cars and caravans. The people who have paid money for these goods are often left out of pocket due to items being non-existent.

Online auctions and marketplaces have become a very popular way of trading online, and fraudsters are using them to take advantage of your trust to sell poor-quality or non-existent items.



You may find that something you've bought online arrives late or never at all. In some cases the products you've paid for are less valuable than shown in the advert, different from the original description, or you weren't told crucial information about the product or terms of the sale.

We also have reports of sellers sending items in the post and never receiving the funds for them. In short, people can be targeted for being a buyer or a seller online.

Reporting to Action Fraud enables intelligence to be gathered, the police to catch criminals and preventative action to be taken. For example, suspending fake websites used to commit online shopping fraud.

By taking some simple steps, you can avoid falling victim in the future.

Top Tips:

- 1. When you're making a payment online, you'll be asked for the 3 digit security (CVV) number on the back of your card; but you should never be asked for your card's PIN or any internet banking passwords
- 2. If you are buying something online that costs between £100 to £30,000 credit cards offer an increased consumer protection over debit cards. So use a credit card when you can
- 3. If you are unfamiliar with a website you want to buy from, do some research first and look for ratings and reviews from customers. Always be cautious about offers that seem too good to be true
- 4. Check the items description carefully and ask the seller any questions if you are unsure of anything
- 5. Never pay by money transfer use a recognised service such as PayPal which protects your money if you have any problems with the seller.



Be suspicious if:

- The buyer or seller has a bad feedback history or has only recently set up a new account to avoid a poor reputation
- You get a private message or email offering you to buy below the current bid or reserve price
- You find an expensive item for sale at an incredibly low starting bid. If an offer seems too good to be true it probably is!

Under-reporting is a real issue with these sorts of crimes as victims wrongly believe they would be wasting our time, there's nothing that can be done or they feel embarrassed by what has happened.

We urge anyone who may have experienced this situation to report it to Action Fraud on 0300 123 2040 or at www.actionfraud.police.uk

Advance Fee Fraud 24.05.2023

What is Advance Fee Fraud?

Advance fee fraud occurs when fraudsters ask victims to make advance payments upfront for goods, services and / or financial gains that do not materialise. Fraudsters contact victims through mail, phone, email and social media.



Examples of Advance Fee Fraud:

- You've won a cash prize or a lottery jackpot and in order to claim the money you must send a payment as a release fee.
- You have started a new relationship online with someone and they invent a reason for cash, using the emotional attachment you have built with them to get you to send money.
- You are a would-be tenant and are tricked into paying an upfront fee to rent a property that doesn't exist.
- You are contacted by someone who says they are from HMRC and you are owed a tax rebate, but you have to pay a fee in order to receive it.
- You are told someone very rich has died and you are in line to receive a huge inheritance, but you have to pay taxes, legal fees or banking charged to have the funds released.
- When someone has been a victim of fraud in the past, they are sometimes contacted again by fraudsters. They pretend to be the Government, Police or a Fraud Recovery Company offering to help recover the money that was lost, but ask for a fee to get it back.





Criminals ask for upfront, refundable fees as a deposit to release a loan or unexpected prizes/goods. They use pressure tactics to get you to pay quickly by bank transfer or even with cryptocurrency.

Question requests for money to release a loan or unexpected prizes/goods. Could it be fake? If you think you've fallen for a scam contact your bank immediately and report it to Action Fraud.



How to protect yourself:

- 1. Never send money to someone that you have never met in person.
- 2. If the promise seems too good to be true, it probably is.

Under-reporting is a real issue with these sorts of crimes as victims wrongly believe they would be wasting our time, there's nothing that can be done or they feel embarrassed by what has happened.

We urge anyone who may have experienced this situation to report it to Action Fraud on 0300 123 2040 or at www.actionfraud.police.uk

24.05.2023 Boiler Room Fraud / Investment Fraud

What is financial investments fraud?

There are many different types of investment fraud. They usually involve criminals contacting people out of the blue and convincing them to invest in schemes or products that are worthless or do not exist. Once the criminals have received payment, they cease contact with the victim.

The majority of investment frauds are run out of offices known as **boiler** rooms.



How to protect yourself from Financial Investment fraud:

- **1. Investment opportunities:** Don't be rushed into making an investment. Remember, legitimate organisations will never pressure you into investing on the spot.
- **2. Seek advice first:** Before making significant financial decisions, speak with trusted friends or family members, or seek professional independent advice.
- **3. FCA register:** Use the Financial Conduct Authority's (FCA) register to check if the company is regulated by the FCA. If you deal with a firm (or individual) that isn't regulated, you may not be covered by the Financial Ombudsman Service (FOS) if things go wrong and you lose your money.

For more information about how to invest safely, please visit: https://www.fca.org.uk/scamsmart

What to do if you've been a victim of Financial Investment fraud:

You could be targeted again: Fraudsters sometimes re-establish contact with previous victims claiming that they can help them recover lost money, this is just a secondary scam. Hang up on any callers that claim they can get your money back for you.

Identity theft: If you suspect your identity may have been stolen, you can check your credit rating quickly and easily online. You should do this every few months anyway, using a reputable service provider and follow up on any unexpected or suspicious results.

Legal advice: In many cases of fraud there is a close correlation between what may be considered fraud and the civil tort of deceit and/or breach of contract, for which there are civil litigation options. We would always advise that you seek professional legal advice or contact Citizens Advice to understand your options.

You can also contact the Financial Conduct Authority's consumer helpline on 0800 111 6768 or report suspicious businesses or individuals by using the reporting form on their website.

Useful links: Citizens Advice www.citizensadvice.org.uk/

Financial Conduct Authority (FCA) www.fca.org.uk



Under-reporting is a real issue with these sorts of crimes as victims wrongly believe they would be wasting our time, there's nothing that can be done or they feel embarrassed by what has happened.

We urge anyone who may have experienced this situation to report it to Action Fraud on 0300 123 2040 or at www.actionfraud.police.uk

Fraud recovery fraud 24.05.2023

Gloucestershire Constabulary are working in partnership with your GP Surgery to share Fraud Prevention Advice on a regular basis.

What it is a Fraud Recovery Scam?

When someone who has been a victim of fraud in the past is contacted again by fraudsters. They pretend to be a government, police or law agency

that can help recover the money that was lost, but <u>ask for a fee</u> to get it back.

How to protect yourself from a Fraud Recovery Scam:

- Be ready for fraud recovery scams if you've been a victim in the past. Challenge any calls, letters or emails from people you don't know or companies you've never contacted
- If you're asked to pay, or give your bank account details, end all contact
- 3. Ask how they found out that you had been a victim. Any report of fraud is protected by law and can't be shared with anyone else outside of law enforcement agencies.



Spot the signs

- You're contacted by an agency that knows a lot about the money you lost, but they want a fee first. Genuine agencies never ask for fees to recover money lost to fraudsters
- They've contacted you with a web-based email address, such as @Yahoo or @Hotmail. Genuine government or law enforcement agencies and law firms don't use webmail
- They've made their email look genuine by including graphics and using official-sounding language.

How it happens

If you've been a victim of fraud in the past, whoever took your money may keep your contact information and contact you again.

This time, they'll pose as an organisation that has been made aware of your loss. They'll claim they can arrest the fraudster, or even recover the money

you lost. In either case, they say you'll need to pay a fee first. This is a form of <u>advance fee fraud</u>; and you'll never get any of the money back.

If you do make a payment, they'll keep coming back to you with another cost that has to be paid, before your money can be returned.

If you ask them to take the fees from the money they claim to have recovered, they will give reasons why this isn't possible. For example, they might tell you that your money is under the control of a court and can only be paid back to you by them.

The fraudsters may also ask you to provide details of your bank account so they can pay your money into it. They will use this information to empty your account.

How to report it

If you've given the fraudsters your bank account details, alert your bank immediately and report the incident to Action Fraud.

Under-reporting is a real issue with these sorts of crimes as victims wrongly believe they would be wasting our time, there's nothing that can be done or they feel embarrassed by what has happened.

We urge anyone who may have experienced this situation to report it to Action Fraud on 0300 123 2040 or at www.actionfraud.police.uk