Introduction – Post 1	Gloucestershire Constabulary are working in partnership with your GP Surgery to share Fraud Prevention Advice on a regular basis. The Economic Crime Team, at Gloucestershire Constabulary work closing with Action Fraud and the National Fraud Intelligence Bureau (NFIB) and are always looking for ways to share information about current fraud trends and how to keep the public safe. We receive hundreds of reports from Action Fraud on a monthly basis from individuals in Gloucestershire who have unfortunately been a victim of fraud. **TAKE FIVE TO STOP FRAUD** Criminals are experts at impersonating people, organisations and the police. They spend hours researching for their scams, hoping that individuals will let their guard down for just a moment. Stop and think, it could protect you and your money.  **STOP** Taking a moment to stop and think before parting with your money or information could help to keep you safe. Reach out to a family member or friend if you have had a call or interaction you are suspicious of, or if something seems too good to be true it may be worth seeking a second opinion from someone that you trust. **CHALLENGE** Could it be fake? It is okay to reject, refuse or ignore any requests or phone calls from numbers you do not recognise or from people you do not know. Remember, only criminals will try to rush or panic you into making financial decisions. **PROTECT** Contact your bank immediately if you think you have been a victim of a scam and report it 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 in this situation to report it to Action Fraud on 0300 123 2040 or at www.actionfraud.police.uk
Energy Rebate - Post 2	Gloucestershire Constabulary are working in partnership with your GP Surgery to share Fraud Prevention Advice on a regular basis. **Beware Energy Rebate Scams** Local residents are reporting that they are being targeted with scam messages about the Energy Bills Support Scheme. The messages state that you can claim a rebate for your energy bills, and instruct you to click a link within the message, to "apply" for the rebate. This takes you to a phishing website whereby you enter personal details, which are then stolen by the fraudsters. There is no need to apply for the Energy Bills Support Scheme and you'll never be asked for your bank details. Under the scheme, households will receive a £400 discount on their energy bills via six instalments, starting in October.  Find out more at https://www.gov.uk/government/news **Links to fake websites** Fraudulent emails and texts containing links to fake websites are hard to spot because they look so realistic – the message may be

	almost the same as you'd receive from the company and may even include the official logos. **So what can you do to protect yourself?** 1. Always take a moment to stop and think before you give out any information. This simple action could save you hundreds – or even thousands – of pounds. Remember, a genuine firm will never pressure you into an immediate decision. 2. Don't click on any links sent to you out of the blue, even if it looks legitimate. Go to the official website for the information, or for the correct contact details to get in touch yourself. 3. Never agree to work by anyone who knocks on your door uninvited, or phones you out of the blue. If you want work done on your home, go to the relevant trade association website or local good trader scheme – your council's website is a good place to start. Or get recommendations from friends and family members. 4. Don't be afraid to be impolite. If you're at all suspicious about a caller, you are well within your rights to shut the door on them or hang up the phone. **The Friends Against Scams website can help give you the skills and confidence to spot scams, and to help protect others. Visit www.friendsagainstscams.org.uk for more information.** Above all, it's important to look after yourself, your loved ones and neighbours. Anyone can be vulnerable due to their situation or circumstances, so we all need to stay alert. Talk about scams and share information. If you think you have been a victim, report it to Action Fraud at **www.actionfraud.police.uk** or by calling **0300 123 2040.**
WhatsApp Scam Messages – Post 3	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**
Computer Software Service Fraud – Post 4	Gloucestershire Constabulary are working in partnership with your GP Surgery to share Fraud Prevention Advice on a regular basis. Viruses are a type of malicious software that can harm devices such as computers, laptops, smartphones and tablets. Once your devices have been infected, this **mal**icious soft**ware** (also known as **malware**) can steal your data, erase it completely, or even prevent you from using your device. Devices can become infected by accidentally downloading an email attachment that contains malware, or by plugging in a USB stick that

	is already infected. You can even get malware on your device from visiting dodgy websites. **Top Tips:** 1. Always use anti-virus software on your laptops and computers. 2. Only install apps and software from official stores such as Google Plan and Apple App Store. 3. If you receive a phone call offering help to remove viruses and malware from your computer, hang up immediately. This is an extremely common scam being seen in Gloucestershire at the moment. 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**
Strong Passwords - post 5	Gloucestershire Constabulary are working in partnership with your GP Surgery to share Fraud Prevention Advice on a regular basis. **How can your passwords be stolen?** Criminals will use the most common passwords to try and access your accounts, or use information from your social media profiles to guess them. If they are successful, they will use the same password to try and access your other accounts. **Create strong passwords:** 1. **Avoid using predictable passwords such as dates, family and pet names**. And avoid common passwords that criminals can easily guess like Password1. 2. **Don't reuse the same password across multiple accounts.** You wouldn't have one key for your car, house and garage. Make sure you have different passwords for any social media account, your emails and any banking apps you might have. 3. To create a memorable password that's also hard for someone else to guess you can combine **three random words** to create a single password. For example **GreenClockFish**.

	 If you suspect your password has been stolen, you should change it as soon as possible. If you have used the same password on any other accounts, you should change the password on these as well. 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 Fraud – post 6	Gloucestershire Constabulary are working in partnership with your GP Surgery to share Fraud Prevention Advice on a regular basis. Online shopping fraud is the number one reported fraud type at the moment across the UK. 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. 

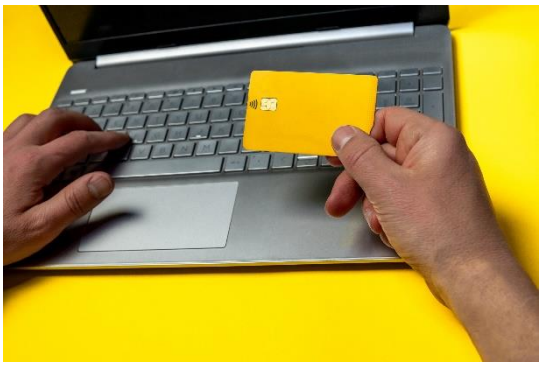
You may find that something you've bought online arrives late or never at all. In some cases the products you've paid for are less valuable than shown in the advert, different from the original description, or you weren't told crucial information about the product or terms of the sale. We also have reports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

It is difficult for police to investigate every instance of fraud – prevention and protection is a far better method of dealing with it. 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**