|  |  |
| --- | --- |
| **Courier Fraud – Post 1** | Gloucestershire Constabulary are working in partnership with your GP Surgery to share Fraud Prevention Advice on a regular basis.  **What is Courier Fraud?**  Courier fraud occurs when people are duped into handing over money or valuables to criminals posting as couriers. Using a variety of different tactics, usually involving the impersonation of policing officers or bank staff, criminals call potential victims and convince them to withdraw a sum of money and hand it over to a courier who is sent to their home address. They may even convince people to hand over their bank cards, PIN’s, as well as high value items such as jewellery, watches and electronic devices.  Courier fraud is one of the highest reported fraud types in Gloucestershire. With an average age of victims being 78 years old, and losing on average £9,000.  **Things to remember:**   1. Your bank or the police will **NEVER** ask you to verify your personal details or your PIN number. 2. Your bank or the police will **NEVER** send a courier to your home address to collect cash, bank cards or PIN’s or any other valuable goods. 3. The police will **NEVER** contact you out of the blue and ask you to participate in an investigation that requires you to withdraw money from your bank, or to purchase high value goods such as jewellery or gold.   K:\Cheltenham\CID\Economic Crime Team\Danielle Sharples\Fraud Protect\Courier Fraud May 2022\Courier-fraud-1-(English).jpg  **STOP** – Taking a moment to stop and think before parting with your money or information could keep you safe.  **CHALLENGE** – Is this person really who they say they are? Could their number be spoofed? It’s okay to refuse any requests for financial or personal details.  **PROTECT** – Contact your bank immediately if you think you may have been targeted, and report the scam to action fraud.  Don’t assume a phone call is authentic just because someone knows your name and address.  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**](http://www.actionfraud.police.uk/) |
| **Advance Fee Fraud - Post 2** | Gloucestershire Constabulary are working in partnership with your GP Surgery to share Fraud Prevention Advice on a regular basis.  **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.  K:\Cheltenham\CID\Economic Crime Team\Danielle Sharples\Fraud Protect\Pictures\July Social Media\4 July - FacebookTwitterLinkedIn.gif  **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.   **How to protect yourself:**   1. Do not send money to someone that you have never met in person. 2. If the promise seems too good to be true, it probably is.   K:\Cheltenham\CID\Economic Crime Team\Danielle Sharples\Fraud Protect\Pictures\July Social Media\18 July - FacebookTwitterLinkedInInstagram.jpg  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**](http://www.actionfraud.police.uk/) |
| **Phishing – Post 3** | Gloucestershire Constabulary are working in partnership with your GP Surgery to share Fraud Prevention Advice on a regular basis.  **What is Phishing?**  Phishing is when criminals attempt to trick people into doing ‘the wrong thing’ such as clicking a link to a fake or dodgy website.  Phishing can be conducted via a text message, social media, and email or by phone. Criminals send phishing emails to millions of people asking for sensitive information such as bank details or which contain links to website which may be harmful to the victim’s devices.  **Top Phishing Protection Tips:**   1. Review your privacy settings on social media and think about what you post online. 2. Is the email addressed to you by name or does it refer to ‘valued customer’, ‘friend’ or ‘colleague’. This can be a sign that the sender does not actually know you, and that it is part of a phishing scam. 3. Sometimes the emails will look like those from official companies, is the design and quality what you would expect? Double check the senders email address, does it sound legitimate? 4. If the email contains threats asking you to act urgently, such as ‘send these details within 24 hours’ or ‘click here immediately’ take the time to think and get a second opinion from someone you trust before taking any action. 5. If it sounds too good to be true it probably is!   If you receive an email which you are unsure about, forward it to the National Cyber Security centres suspicious reporting service at [report@phishing.gov,uk](mailto:report@phishing.gov,uk) this may help other people from being affected.  If you have already clicked onto a link – do not panic. Follow these three simple steps to keep yourself and your details safe.  **Step 1**: Open your anti-virus software and run a full scan on your device. And then follow any instructions given to you.  **Step 2**: If you have been tricked into providing your passwords you should change your passwords on your accounts as soon as possible. Make it as strong as you can – we recommend using three random words. For example “OrangeKettleTree” the more complex the better e.g. Or%nge.K3ttl3.Tree52  **Step 3**: If you have lost money, you need to report this to Action Fraud and to your bank straight away.  K:\Cheltenham\CID\Economic Crime Team\Danielle Sharples\Fraud Protect\Pictures\August Social Media\4 August - FacebookTwitterLinkedIn.gif  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**](http://www.actionfraud.police.uk/) |
| **Banking and Credit Card Fraud – Post 4** | Gloucestershire Constabulary are working in partnership with your GP Surgery to share Fraud Prevention Advice on a regular basis.  **What is Debit and Credit Card Fraud?**  Debit and Credit Card Fraud happens when personal information is stolen from your debit, credit or store cards, or even the card itself may be stolen. The card is then used to purchase items using money from your account, either online or via contactless payments.  **How can I protect my card and banking information?**   1. Look after your cards. Keep them with you wherever you go, and do not hand them over to anyone. 2. Be protective of your banking information. Either store your statements, receipts and documents safely or destroy them using a shredder. 3. Do not keep a copy of your PIN with your debit or credit cards. This includes keeping a note in your purse or wallet or writing the PIN directly on your cards. 4. Sign new cards as soon as they arrive and cut up old cards through the magnetic strip and the chip once they have expired or been cancelled. 5. If you have lost or misplaced one of your cards, call your bank immediately to have the card stopped. This will ensure that no unauthorised transactions will take place.   K:\Cheltenham\CID\Economic Crime Team\Danielle Sharples\Fraud Protect\Pictures\Take 5 Leaflets\6485_TakeFive_A_15e_MPU_300x250px.jpg  **What should I do if I have been a victim of bank card fraud?**   1. Immediately report your card as lost or stolen with your bank. You should be able to find a 24-hour emergency contact number on one of your statements or by searching on the company website. 2. Call your bank if you have any transactions on your statement or internet banking that you do not recognise. 3. Consider contacting CIFAS, the UK’s Fraud Prevention Service to apply for protective registration. Once registered, CIFAS will carry out additional checks whenever anyone applies for a financial service for example a loan, credit card or finance using your name and address.   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**](http://www.actionfraud.police.uk/) |
| **Romance Fraud Red Flags - post 5** | Gloucestershire Constabulary are working in partnership with your GP Surgery to share Fraud Prevention Advice on a regular basis.  **What is Romance Fraud?**  Dating and meeting new friends online is one of the most popular ways for people to meet. With millions of people finding new friendships, relationships and love in this way. Unfortunately, amongst the genuine profiles there are fake profiles set up by fraudsters. They are masters of manipulation, playing on your good nature and emotions to ultimately steal your money.    **Romance Fraud Red Flags:**   * The person you are speaking to lives or works overseas. * Jobs including the military, oil rig worker, any medical professionals (surgeon/doctor), United Nations employee are often used by fraudsters. * Any mention of a high value box, this could include money, gold bars and jewels. Scammers often say it is inheritance, wages or found treasure. * Moving your conversation to Google Hangouts or WhatsApp. * Asking you for any kind of money this includes gift cards or Bitcoin currency. * They cannot video call you with a crystal clear image. There is **no** reason someone cannot video call with a clear image and in sync audio with the technology we now have available. * Any sob stories. If the person you are speaking to claims to be a struggling single parent, widowed, hungry, homeless or stranded in a foreign country. * Declaring their love for you very early on or introduce the subject of marriage. * Claim to have had the same experiences or values as you. If you tell them you are divorced they will tell you they are as well. If you are religious, they will lie and say they share your faith. * Promise to meet you but will always have an excuse why they cannot. * Watch out for grammar and spelling. English is likely not their first language.   **How can I protect myself whilst online dating?**   * Always check their social media page. Was it created recently? Do they have only a few friends/followers? Do they only have a few photos? Is yes, this is indicative of a fraudster. * Do not take any excuses why they cannot video call. If they claim to work in a secure area then they need to call against a plain wall where no sensitive material can been seen. If it is truly that secure of a place they would not be allowed phones in the first place. * Do not accept anything less than a perfect picture and sound on a video call. Scammers have tricks to fool you. During the call ask them to touch their eye and then their head. * Tell a family member or a friend about your love interest. An impartial person will spot any red flags that you might miss. * No relationship should ever involve you having to send money. * Reverse image search any photos. It could tell you where else on the internet the image is   Following these tips should help keep you safe when speaking to new people online. For more information on Romance Fraud please visit the Action Fraud Website.  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**](http://www.actionfraud.police.uk/) |
| **Romance Fraud – post 6** | Gloucestershire Constabulary are working in partnership with your GP Surgery to share Fraud Prevention Advice on a regular basis.  **What is Romance Fraud?**  Dating and meeting new friends online is one of the most popular ways for people to meet. With millions of people finding new friendships, relationships and love in this way. Unfortunately, amongst the genuine profiles there are fake profiles set up by fraudsters. They are masters of manipulation, playing on your good nature and emotions to ultimately steal your money.  Fraudsters are often very flattering, appearing very interested in you but will always have a number of excuses as to why they cannot meet you in person.  **How can I protect myself?**   1. Keep all communication on the dating website or app you are using. 2. Do not be convinced by profile pictures, these may have been taken from elsewhere on the internet. You can check photos using a reverse image search on the internet through websites such as <https://www.tineye.com> or <https://reverse.photos>. 3. Do your own research on the person you are speaking to. Are they on any social media? Can you confirm what they are telling you to be true, such as where they live or where they work? 4. Never send money to someone you have not met in person. 5. Be wary of anyone asking you to received money on their behalf and asking you to transfer it on. They may be using you to launder money. 6. Talk to your friends and family for advice, even if the person you are speaking to online is asking you to keep the relationship or friendship a secret.   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**](http://www.actionfraud.police.uk/) |