

Fraud Prevention Talk Summary

Our September 2026 monthly talk was given by Rhiannon Parker of Gloucestershire Constabulary's Cyber Crime and Fraud Unit, and covered ways in which we can help ourselves to avoid becoming a victim of fraud.

National statistics say that fraud now comprises nearly 50% of all crime committed and the volume of fraud reported to the police is significantly understated. Last year alone nearly £15m of fraud was reported in Gloucestershire so if you have been a victim you are not alone.

Fraud often goes unreported as fraud victims feel embarrassed, or that it was their fault or that nothing will happen. There is nothing to be embarrassed about – fraudsters are professionals whose job is to get money from victims. They use clever techniques and scripts to build trust with their victims and they do this all day long. Victims are inexperienced and potentially vulnerable but there are things you can do to be more fraud aware.

The 'golden rule' of fraud protection is:

Stop! Think!

- Is the contact (email, text message, phone call etc.) unexpected? You can always ignore the first contact, if they are legitimate and really need to speak to you, they will contact you via a different route.
- How do I know they are who they say they are? If you're not sure of the identity then check the sender's email address or put the phone down, wait for 5 minutes and then ring a publicly available contact number for the organisation they say they are from. You can also ring 159 to get direct access to any bank's fraud department.
- What information are they asking me to disclose? Banks and other legitimate organisations will never ask you to disclose your PIN number, passwords or other sensitive information.
- Am I being rushed to comply? Fraudsters use time pressure to deter victims from asking too many questions or thinking about the possibility of fraud. Legitimate callers will not put you under pressure by saying something is 'urgent' or 'critical'.

If you have any suspicions then ask a friend or family member if they think the contact is legitimate. If you are still not certain, don't respond to the contact. Legitimate organisations will contact you again, fraudsters won't.

Whilst not directly related to fraud, don't forget that most banking apps will let you freeze your debit or credit card should you misplace it or think it may have been stolen. You can then unfreeze it if the card turns up.

A lot of fraud is what is known as 'cyber crime' i.e. carried out via a computer, tablet or mobile phone. Here are some tips to lessen the chances of being a victim of cyber crime:

- Your email password is the gateway to accessing information about you – make sure it is a strong password and don't use the same password for other applications.
- Create a strong password - the best ones are three random words (not family names, or addresses) e.g. 'cactusbicyclepants'. Even stronger if you incorporate capital letters, numbers and special characters such as 'C4ctusBicyc1epant\$'.
- Using password manager applications to remember passwords on your phone, tablet or PC is OK as long as the device is protected with biometric recognition or at least a PIN. If you feel safer writing down passwords in a book, that is fine but make sure the book is not kept anywhere near the computer or device that the passwords are used for.
- Always use two-factor authentication when it is offered by the organisation. This is where you sign into something and it then sends you a code by text or email which you also have to enter. Slightly less convenient for you but impossible for a fraudster to circumvent unless they have access to more than one of your devices.
- 'Passcodes' are also becoming popular as a way of signing into online accounts – these will only work on one specific device so unless the fraudster has access to your device and the passcode they can't get access.
- Think about letting a family member know the PIN for your phone so if you are ever incapacitated they have access to your online information. If you use facial or fingerprint recognition on a device it will default to a PIN number after a number of unsuccessful attempts.
- Keep software and devices up to date by using the latest version of software/applications – the latest version will always be the most secure.
- If you don't use 'cloud' storage e.g. Google drive, Onedrive or iCloud, take a regular backup of data from your device onto a memory stick. Should you ever be locked out of a device you won't lose all your precious photos and other data. Ideally give a copy of the backup data to a family member for safe-keeping just in case you were to lose your memory stick.

If you need help with any of the above, our u3a Tech Support group can help you with all of these preventative measures. We meet on the second Thursday of each month at The Royal Oak from 10:30-12:00 – just drop-in with your device.

Other useful resources:

<https://stopthinkfraud.campaign.gov.uk/>

<https://www.reportfraud.police.uk/>

<https://www.ncsc.gov.uk/section/advice-guidance/you-your-family>

<https://cfeu.org.uk/glassjar/>