Summary of the General Meeting on Scams

Scammers use greed, fear and urgency to catch their victims.
They piggy-back on current issues/stories (e.g. winter fuel allowance)
If it seems too good to be true, it probably is.
If something is unexpected, treat it with great caution - **THERE IS NO RUSH!**

Phone scams:

Banks rarely call you. Call them back rather than take them at face value.
If called by someone pretending to be from your bank and you are unsure, STOP, HANG UP, CALL 159. 159 will get you through to your bank (after some Q&A).
Scammers can get a lot of information from you using identity confirmation.
Make sure that you disconnect the phone from a scam call before calling your bank, as the scammers could still be on the line and could answer pretending to be the bank. Call someone else first to ensure that the line is clear, or use another phone.

Cold Callers:

Doorstep sellers can be checking you out for follow-up burglary.
Nottingham knockers – there is no licensed scheme for released prisoners. They work for criminal gangs.

Emails and texts:

Don't open suspect links or attachments in emails and text messages.
Check email addresses and links for obvious errors (no connection with the supposed firm) or subtle differences (misspellings).
Don't enter any login or account details on a screen accessed via a received link – look for the authentic website independently.

Romance Fraud (currently rife)

Romance frauds happen when the victim thinks they've met the perfect partner through an online dating website or app, but the other person is using a fake profile to form a relationship with them. They're using the site to gain the victim's trust and eventually ask them for money or enough personal information to steal their identity.
Romance fraudsters are masters of manipulation and will go to great lengths to create a false reality in which an individual feels that they are making reasonable and rational decisions.
The challenge for many family and friends of romance fraud victims is being able to disrupt the false reality created to enable the victim to see the situation for what it really is - a fraud.
This type of crime is happening increasingly often and losses often amount to thousands of pounds.
There is no fool like an old fool…!

Identity theft

Be careful about throwing out documents with personal information – shred or burn anything sensitive.

Online security:

Use antivirus protection on your PC.

Microsoft Defender (free with Windows) should be adequate for normal online purposes. Use something more industrial-strength if you are concerned or do a lot of sensitive transactions or hazardous browsing.
https://haveibeenpwned.com/ - shows if your email account and password have been acquired from data protection breaches. Change your password if it appears.
https://haveibeenpwned.com/Passwords - does your password appear? If so, change it!

S – STOP! There is no hurry. If it is genuine there will be a follow-up.

C – CHECK, consult, consider, call a friend.

A - ASK for ADVICE. Citizens Advice, CIFAS *0808 223 1133* https://www.cifas.org.uk/contact-us/i-want-help-or-advice-on-scams

M - Mention to others, report to Action Fraud **0300 123 2040** **https://www.actionfraud.police.uk/**
https://www.ncsc.gov.uk/collection/phishing-scams/report-scam-email
https://www.ncsc.gov.uk/collection/phishing-scams/report-scam-text-message
https://www.ncsc.gov.uk/collection/phishing-scams/report-scam-call
https://www.ncsc.gov.uk/collection/phishing-scams/report-scam-website

Some tools:

https://www.ask-silver.com/ is an app that checks WhatsApp messages
https://www.trendmicro.com/en_us/forHome/products/trend-micro-check.html
https://www.takefive-stopfraud.org.uk/
https://www.ageuk.org.uk/information-advice/money-legal/scams-fraud/
Ironically https://www.scamadviser.com/ has been hit with a data protection breach!