Safeguarding Adults Week - Fraud and Scams

Vulnerable people can be more at risk to fraud and scams therefore can be a financial abuse issue (as well as other types of abuse). Clair Kelland Detective Chief Inspector, South West BCU Safeguarding Hub has shared some information regarding this important issue.

Top Fraud types reported to Action Fraud

Online Shopping
Victims are convinced into paying money for items that don't exist or are counterfeit when shopping online. Stick to the terms and conditions of the website, don't pay via direct bank transfer.

Advance Fee
Victims are encouraged to pay an advance fee with the promise of a larger amount back in return. E.g. a scam email from "HMRC" requesting an admin fee for taxes owed. Contact the company directly to check (on a number you know to be correct)

Investment Fraud
Victims are pressured into making "investments" that don't actually exist or have no chance of the financial return suggested. Genuine investment companies do not cold call people.

Door to Door / Bogus traders
Fraudulent builders convince victims to pay for work that doesn't need doing or charge amounts far exceeding the cost of work. Genuine builders do not call door to door, use a trusted, verified and reviewed trader.

Payment Fraud
(aka Mandate fraud) When transactions between genuine seller and consumer are intercepted or spoofed and payment details are altered to an account controlled by the fraudster. Double check requests for money, especially if bank account details have changed. Contact the person directly.

Romance Fraud
Online dating fraud, fraudster gains the affections of the victim and use this to convince them to send money often as a "loan" due to unforeseen circumstances.
Stay on the website to talk (don't give out personal email and telephone number), don't give money to people you haven't met.

Computer Software Fraud
Fraudsters pretend to be computer engineers offering to "fix" victims computer over the internet. Download software to compromise their online banking / personal data or charge extortionate amounts. Your internet / telephone provider does not monitor your computer or internet, they will not cold call you to tell you there's a problem.

Courier Fraud / Push Payment (Impersonation scams)
Victims are called by fraudsters pretending to be police, HMRC or from the victim's bank and convince them to give their card details over the phone or pay a fine to avoid arrest. Or in some cases, transfer money to a "safe account" buy gift vouchers or to go and withdraw money as part of an "investigation." The fraudsters arrange for a courier to pick up the victim's card or cash to take it away for "evidence". Your bank or the police, will never ask you for your password, PIN or to attend your bank, withdraw, transfer or pay money over the phone or send couriers to collect your card or cash. Nor would they ask you to buy goods or vouchers. This is a scam.

The tax office (HMRC) do not leave voicemails and do not threaten arrest over the phone.

Please watch our video; https://youtu.be/fy-RSQfwLDw for more information.

Remember, criminals can spoof their number, i.e. they can change their number to be anything they like, such as the number on the back of your bank card.
Caller ID is NOT proof of identity.

Whenever you get unsolicited contact from a business, take 5 minutes to verify their claims via a trusted method. Never use the number given in an email, text or call.

1. Hang up (Never give details or money following a cold call)
2. Take 5 (Seek a second opinion, tell someone what has happened)
3. Verify (if concerned, contact the company via a pre-confirmed method)

Please help us share this information, tell your family, friends and neighbours as people are still falling victim to these types of fraud.
All of our videos and electronic leaflets can be found on the following website; www.met.police.uk/littlemedia

Always report, Scams fraud and cyber-crime to Action Fraud, either online at www.actionfraud.police.uk or by telephone on 0300 123 2040.

Many door-to-door scams involve the householder being tricked into paying for products or services that are overpriced or of poor quality. An example of this is being approached regarding building or roofing repairs that are not necessary. The scammer may claim that the work is required to be done urgently and they can give you a good deal. They will put pressure on you to have the work done immediately and may ask for payment upfront. Often the work is not completed or if it is to a poor standard. You may also be overcharged for any work done.

Always check the identity of anyone you don't know who attends your home address. Representatives of large companies and organisations should carry id. If you want to check a callers identity do not call the telephone number shown on their id. Find a telephone number for the organisation on the internet or in a phone book and use this to make contact. If you are not happy about a person's identity do not let them in to your house.

Don't be forced into making quick decisions. Scammers may put pressure on you by offering you a take it or leave it deal at the time of their visit, or claim that the repairs have to be done immediately to avoid more expensive future works.

Take time to consider your options and research costs from other providers.
If you feel pressured by a salesperson or are not happy with their behaviour ask them to leave. Be firm as they must leave if you ask them to.

Remember – out of the blue, no thank you.

Legitimate builders do not call door to door.
Never pay upfront for goods or services you have not received.
Don't give out personal information unless absolutely necessary, particularly to someone you do not know or trust

Call the citizens advice consumer helpline following a door step caller, 03454 04 05 06

Follow our top 10 tips for staying safe online.

1. Have a strong password. To create a strong password simply join three random words together. Then add numbers, symbols and uppercase letters. For example: 19fisHboaTtuliP95!!
2. Have an (up to date) anti-virus. Download updates and scan your devices regularly (at least once a week).
3. Update software – install patches. Always update or patch your software as soon as you're prompted to ensure that it remains safe and secure.
4. Back up your data regularly. Regularly copy your important information to external storage like external hard drives, USBs or cloud storage.
5. Don't click on links / open attachments (unless verified) in emails or texts. Clicking on unverified links or attachments in emails or texts can give criminals access to your devices.
6. Set privacy settings on social media. Be careful who can see what you share online, ensure your privacy settings are set to a high level. Never share private information (like your address) on social media.
7. Avoid public Wi-Fi for personal activities. Never use free Wi-Fi for anything you don't want a stranger to see, and consider keeping Wi-Fi turned off unless you need it.
8. Turn on two factor authentication. Where available turn on 2FA on any accounts that contain important or personal information. Go to www.turnon2fa.com for instructions on how to set up 2FA across popular online services.
9. Always question requests for personal information. Criminals will try all sorts of stories to get you to part with your money or data, Never give information to anyone who contacts you out of the blue.
10. Report all fraud and cyber-crime to Action Fraud. Even if you didn't lose money, you should still report every instance of fraud or cyber-crime you're targeted by. Every report assists police investigations, disrupts criminals, and reduces harm.

The following are useful websites for information;

www.met.police.uk/littlemedia
Electronic copies of our leaflets and links to our animations

https://takefive-stopfraud.org.uk
"*National campaign that offers straight-forward and impartial advice to help everyone protect themselves from preventable financial fraud*"
https://www.getsafeonline.org
"*UK's leading source of unbiased, factual and easy-to-understand information on online safety*"
www.haveibeenpwned.com
Enter your email to see if it's ever appeared in a breached website.
www.turnon2fa.com
Step by step instructions on how to activate 2 factor authentication on a large number of websites.

Clair Kelland Chief Inspector
South West BCU Safeguarding Hub