Online Fraud & Cyber Crime

Reporting Fraud

Fraud and Cyber crime is reported nationally to **Action fraud.**

Via phone **0300 123 2040**
Or online
https://actionfraud.police.uk/

Useful Contacts

National Cyber Crime Unit
0370 496 7622
UK Finance
0207 706 3333
Citizens Advice Consumer Helpline
03454 04 05 06

Fraudster Techniques

- **Spoofing:** Making an email/text/call look like it's coming from someone else.
- **Phishing:** Fraudulent emails
- **Smishing:** Fraudulent text message
- **Vishing:** Fraudulent phone calls.

Resources & Advice

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

Email: **cyberprotect@met.police.uk**

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 breach.

www.turnon2fa.com
Step by step instructions on how to activate 2 factor authentication on a large number of websites.

7 Tips to avoid Cyber crime

1. Have a strong password
2. Have an (up to date) anti virus
3. Update software – install patches
4. Back up your data regularly
5. Don't click on links / open attachments (unless verified) in emails or texts
6. Set privacy settings on social media
7. Avoid public Wi-Fi for personal activities

Creating Strong Passwords

1. Three random words
   fish boat tulip
2. Capitalise some letters
   19fis**H**boa**T**tuli**P**95
2. Add some numbers
   19fisHboatTuliP**95**
4. Add special characters
   19fisHboaTtuliP95**!!**

METROPOLITAN POLICE

Fraud Type Summaries

Online Shopping

Victims are convinced in to paying money for items that don't exist or are counterfeit when shopping online.

Advance Fee

Victims are encouraged to pay an advance fee with promise of a larger amount back in return. E.g. a scam email from "HMRC" requesting an admin fee for taxes owed.

Investment Fraud

Victims are pressured in to making "investments" that don't actual exist or have no chance of the financial return suggested.

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.

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.

Stats Overview

37% of all crime has a cyber element. -

Office for National Statistics

UK citizens are 20 times more likely to be defrauded at their computers then held up in the street.

-National Cyber Security Centre

Over-65s are three times more likely to lose money to fraudsters than to be burgled

-Centre for Counter Fraud Studies

Courier Fraud

Victims are called by fraudsters pretending to be police, HMRC or from the victims bank and convince them to give their card details over the phone. 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 victims card or cash to take it away for "evidence".