METROPOLITAN POLICE

FALCON
FRAUD AND LINKED CRIME ONLINE

Stats Overview

- 43.8% 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

Fraudster Techniques

- **Social engineering:** "*The clever manipulation of the natural human tendency to trust*" (hacking the human)
- **Spoofing:** Making an email/text/call look like it's coming from someone else.
- **Phishing:** Fraudulent emails
- **Smishing:** Fraudulent text messages
- **Vishing:** Fraudulent phone calls.
- **Data Leakage:** Fraudsters exploit potential victims transferring personal info to the outside world. e.g. by social media.
- **Ransomware:** Malware that encrypts data, which is then held to ransom.

7 Tips to avoid Cyber crime

1. Have a strong password
2. Have an (up to date) anti virus
3. Update software – 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. Verify requests for payment/bank details

Resources & Advice

www.met.police.uk/fraud

Little Book of Big Scams
Little Book of Cyber Scams
Little Leaflet of Cyber Mistakes
Little Guide Videos

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*"

Creating Passwords

1. Three random words
   fish boat tulip
2. Add some numbers
   19fishboattulip**95**
3. Capitalise some le ers
   19fis**H**boa**T**tuli**P**95
4. Add special characters
   19fisHboaTtuliP95**??**

Useful Contacts

Action Fraud
0300 123 2040

National Cyber Crime Unit (24/7)
0370 496 7622

UK Finance
0207 706 3333

Information Commissioners Office
0303 123 1113

METROPOLITAN POLICE

METROPOLITAN POLICE

FALCON
FRAUD AND LINKED CRIME ONLINE

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.

Card, Cheque & Online banking
Fraud involving banking, e.g. ATM fraud, cloned cards, hacked online bank accounts etc.

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

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.

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.

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.

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.

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".

Reporting Fraud

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

Via phone **0300 123 2040**

Or online **https://actionfraud.police.uk/**

Hints & Tips

1. Out of the Blue? No thank you!
2. Stay on websites and follow their terms and conditions.
3. Seek help/second opinions and search for reviews of sellers/ traders.
4. If something appears to good to be true, then it probably is.
5. Never use direct bank transfers with people you haven't met.
6. Check changes to payment details or addresses via a trusted contact method.