Keeping up with Financial Crime

Alexander Hides

Analyst

NFIB: Serious & Complex Case Team

National Fraud Intelligence Bureau

ActionFraud

National Fraud & Cyber Crime Reporting Centre

actionfraud.police.uk

CITY OF LONDON POLICE

National Policing Lead For Fraud

Action Fraud customer channels

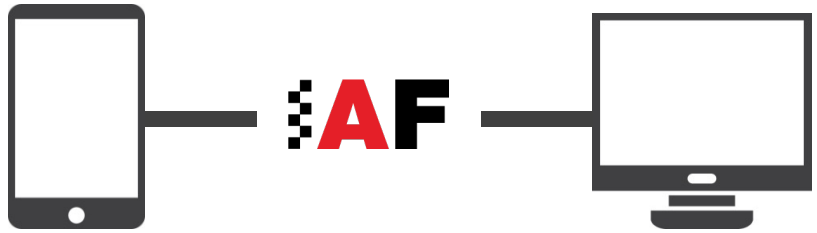
ActionFraud
National Fraud & Cyber Crime Reporting Centre
actionfraud.police.uk

Social Media

Help and advice.
How to protect against fraud.
News and alerts.
Real time fraud intelligence.

National Fraud and Cyber Crime Reporting Centre

700k+ reports per year
2,000+ calls per day
250+ web chats per day



0300 123 2040

Report fraud and cyber crime.
Help, support and advice.

0300 123 2050

If you are deaf or hard of hearing you can contact us on textphone

24/7 Live cyber

Specialist line for business, charities or organisations suffering live cyber attacks

Report 24/7 & Web Chat

www.actionfraud.police.uk
Secure online reporting.
News and Alerts.
Advice on avoiding the latest scams.

POLICE SCOTLAND
Keeping people safe
POILEAS ALBA

Report Fraud in Scotland:
All reports of fraud and any other financial crime should be reported to Police via **101** without delay.

What happens when you report

ActionFraud
National Fraud & Cyber Crime Reporting Centre
actionfraud.police.uk

REPORTING

ActionFraud
National Fraud & Cyber Crime Reporting Centre
actionfraud.police.uk

Secure online reporting and advice on avoiding the latest scams.

actionfraud.police.uk

Report and advice over the phone

0300 123 2040

ANALYSIS

National Fraud Intelligence Bureau

Reports from Action Fraud are analysed by experts with **the National Fraud Intelligence Bureau (NFIB)**, which is run by the City of London Police.

Data matching allows reports from different parts of the country to be linked through analysis, identifying the criminals behind the scams.

INTELLIGENCE, INVESTIGATION AND DISRUPTION

Intelligence helps catch criminals and protects others.

Your reports are sent to local police forces for investigation.

Bank accounts, websites and **phones numbers** used by fraudsters can be disrupted by the NFIB.

Not every report results in an investigation but every report helps to build a **clear picture** making the UK a more **hostile place** for fraudsters to operate in.

Investment Fraud

- Emerging threat to younger victims.
- Commodities of interest include Cryptocurrency or Forex (foreign exchange trading).
- Suspects engaging with victims via social media platforms such as Instagram & Facebook.
- 47% of investment fraud victims where social media was an enabler were aged under 30.

Advance Fee Fraud

Fraudsters claim a fee is required before the victim can secure a job/internship.

1. Exercise caution when asked to pay in advance for an internship or opportunity. Speak to your university who might be able to verify its validity.

2. Ask ‘agents’ which agency they work for. Independently research and contact them yourself using separate details.

3. Contact the organisation purporting to offer the opportunity directly to check it exists.

4. If it sounds too good to be true, it probably is!

CITY OF LONDON POLICE
National Policing Lead For Fraud

National Fraud Intelligence Bureau

Rental Fraud

FY2019/20:

- 8000+ reports
- £24.5m financial loss

- Do not send money to anyone advertising rental properties online until you are certain the advertiser is genuine. If you aren't sure, do not send!
- If you need to secure accommodation in the UK from overseas, seek the help of the employer or university you are coming to, or get a friend, contact or relative to check the property exists and is available.
- Do not pay any money until you or a reliable contact has visited the property with an agent or the landlord.
- Ask for copies of tenancy agreements and any safety certificates such as Gas Electricity or HMO Licence.
- Do not be pressurised into transferring large sums of money. Transfer funds to a bank account having obtained the details by contacting the landlord or agent directly after the above steps have been followed. Be sceptical if you're asked to transfer any money via a money transfer service like Western Union.

CITY OF LONDON POLICE
National Policing Lead For Fraud

National Fraud Intelligence Bureau

“ishing”

Phishing = Emails

Smishing = Text Messages

Vishing = Telephone Calls (voice)

What should you do if you’ve received an email, text or call?

- Do not click on any links.
- Do not reply to the same number or contact the senders using the supplied contact details in any way.
- If you have clicked on a link, do not supply any information on the website that may open.
- Do not open any or download any attachments that arrive.
- If you are expecting communication, respond to any approaches having independently researched contact details online. If called and you’re unsure, tell the caller you’ll contact them yourself.

CITY OF LONDON POLICE
National Policing Lead For Fraud

National Fraud Intelligence Bureau

Money Mules

Money mules enable money laundering, washing the proceeds of crime through a seemingly innocent bank account so that the funds appear legitimate before being sent on elsewhere.

- 1. **Keep control.** Don't give away any of your bank account details, unless you know and trust the person receiving them – and never let anyone else access your account. Alarmingly, nearly one in seven (14 per cent) students have shared their pin number with someone else

  2. **Money for nothing?** Be cautious of unsolicited offers of easy money as this is a common tactic used by criminals to recruit money mules

  3. **Take time to think.** Remember that letting someone else use your bank account is a potentially serious crime which could damage your financial future – is it worth it?

  4. **Too good to be true?** Remember the simple rule of thumb about offers of easy money: if it looks too good to be true, it probably is. Do not transfer funds received from an unknown party or employer to somewhere or someone you don't know.

CITY OF LONDON POLICE
National Policing Lead For Fraud

National Fraud Intelligence Bureau

Questions?

CYBER AWARE

cyberaware.gov.uk

TAKE FIVE TO STOP FRAUD™

takefive-stopfraud.org.uk

National Cyber Security Centre
a part of GCHQ

ncsc.gov.uk

CITY OF LONDON POLICE
National Policing Lead For Fraud

www.actionfraud.police.uk

National Fraud Intelligence Bureau