

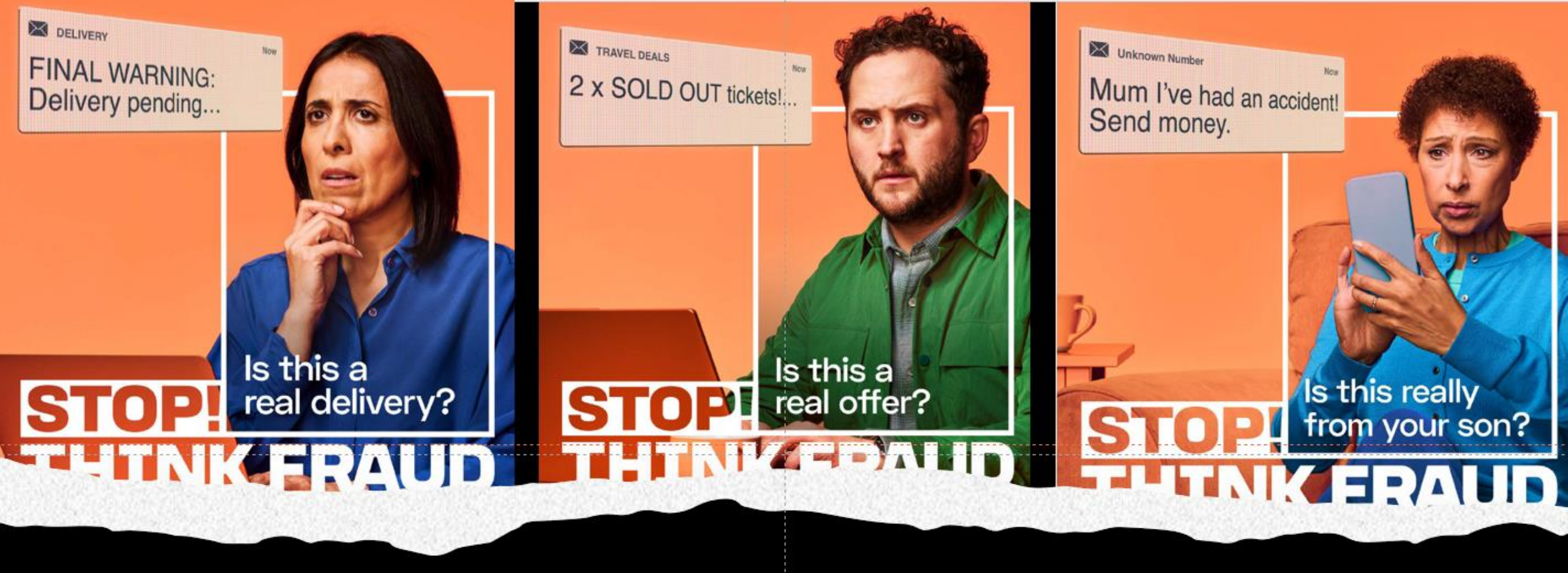
Protecting yourself from fraud & cyber crime

Alan Mordey

Cyber Prevent & Protect Officers
Serious Fraud & Cyber Unit
Hertfordshire Constabulary

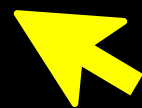
Email: hertscyberprotect@herts.police.uk





Fraud and Cybercrime accounts for 40% of reported crime

<https://stopthinkfraud.campaign.gov.uk>



Social engineering

Criminals attempt to trick users into doing '*the wrong thing*':

- ✗ divulging sensitive/personal information
- ✗ opening/downloading an email attachment – but it's a scam
- ✗ clicking links/visiting a fake website

Scam messaging typically:

1. are from an **authority / organisation / person you heard of.**
2. appeal to your **emotions.**
3. have a sense of **urgency.**
4. are topical / current **events.**

email/online
'Phishing'



text
'SMShing'



phone
'Vishing'



'Quishing'



Call from the Police...



**Be patient with banking staff if they ask you
loads of questions...**



Banking Protocol

Banking Protocol launched in MAY 2017

- Response to Courier Fraud, Rogue Traders, Romance / Dating & Investment frauds.
- Banking staff trained to recognise signs of potential fraud in action.
- Trained to dial 999, and quote 'Banking Protocol'.
- Police response is expected.

Secondary Banking Protocol launched NOVEMBER 2019, whereby bank will contact victim over phone re recent attempted transaction

- If not happy, staff can call victim into branch, payment frozen.
- If branch not happy/you cannot attend, then bank will contact Police who will attend within 72 hours.





FRAUD!

SPOT IT AND STOP IT!



Calls claiming to be the bank or the police



Sudden claims of suspicious banking activity



Being asked for PIN number or passwords



Requests for bank card or cash as 'evidence'



Asked to purchase high-end jewellery and goods



'Couriers' sent to collect card, cash, or bank details

Police or bank officials will never ask for pin numbers, bank cards, goods, money, or request your assistance with an investigation!

To **verify** the caller, hang up the phone and wait 5-10 minutes (criminals may keep your landline open) or use a different phone and call:

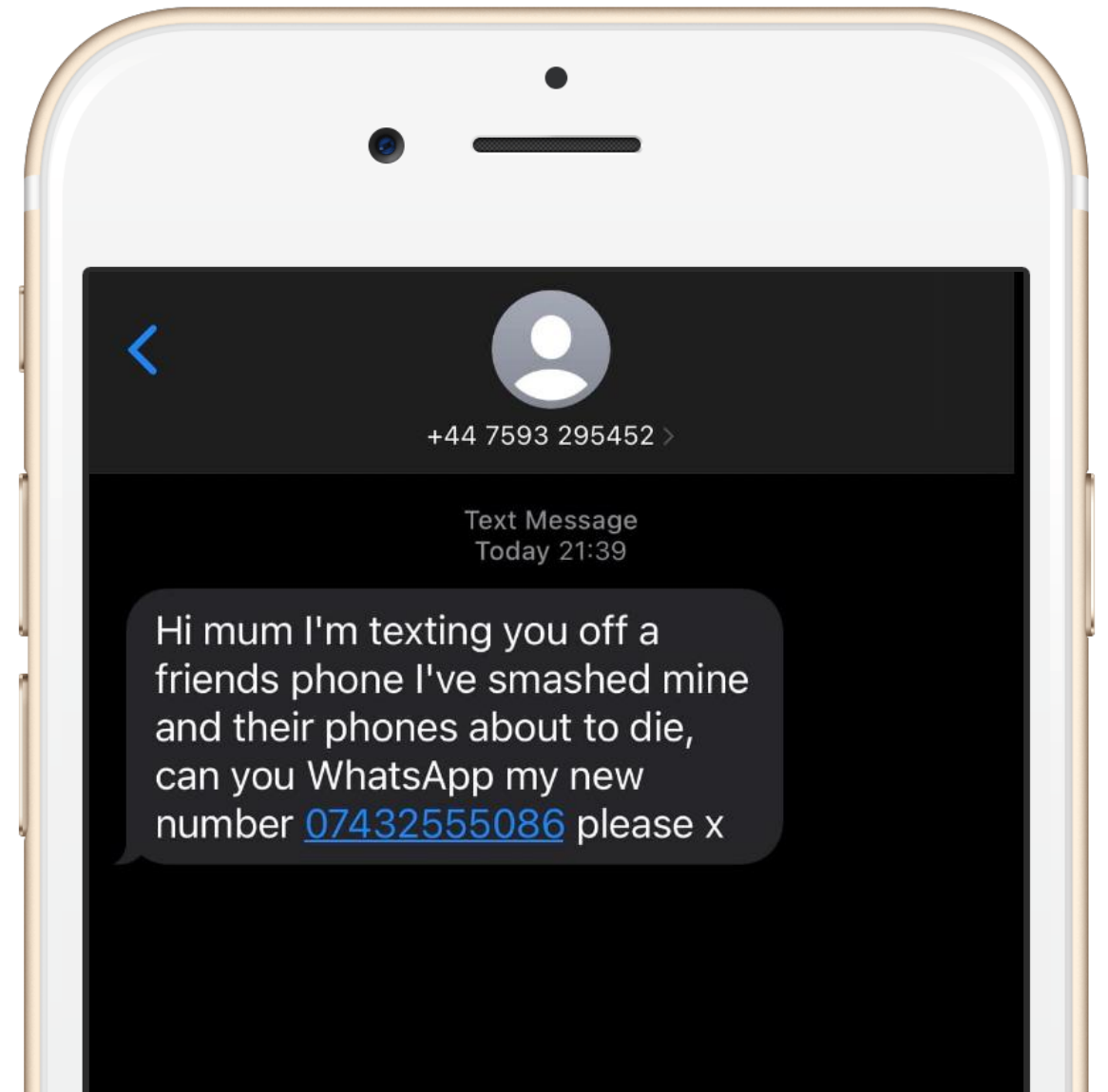
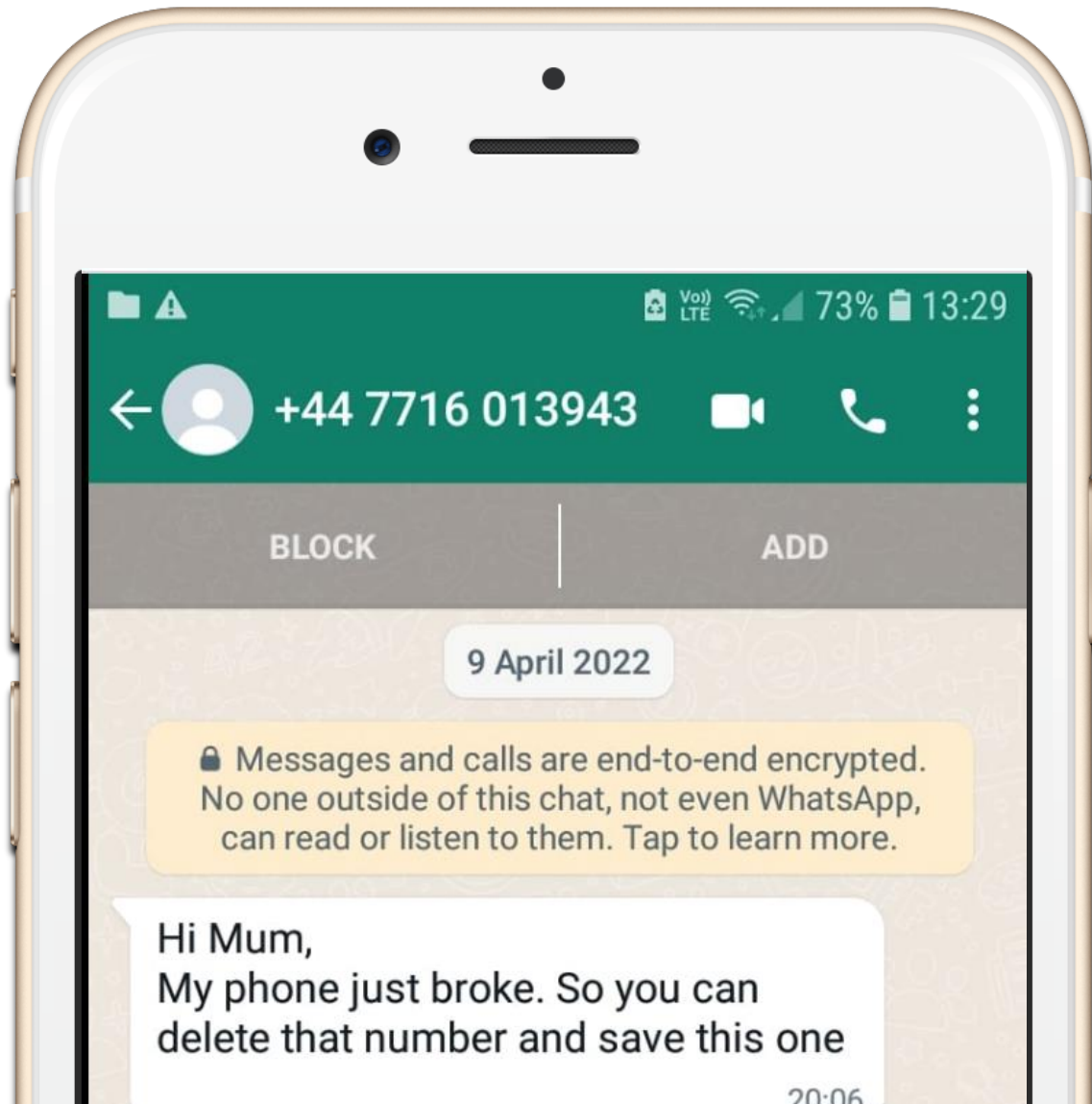
101 - to verify if the person is a police officer.

159 - to speak to your bank (or call the number on the back of the bank card).

Hi Mum...



“Family/Friend in Need” Text Scam



Too good
to be true...

... and it
usually is!

11:05 Sun 28 Jul

43%

facebook

Search



Get your laptop from last year's generation

Sponsored · ⚙️

Tesco is giving away Dell laptops to everyone in the UK due to the end of the warranty period and the need to clear out warehouses and get rid of excess inventory for new models 🖥️
Click on the button and answer 3 questions 📌



Get rich quick!



Investment & Pension Scams

Scammers persuade you to part with your pension/cash:

- promising investment opportunities that are simply **‘too good to be true’**,
- giving false information.

They call several times and could even have details of previous investments you’ve made.

Watch out for:

- Any cold calls out of the blue.
- ‘Loans’, ‘savings advance’ or ‘cashback’ from your pension or talk about new investment techniques.
- Investments in stocks and shares in wine, jewellery, carbon credits or land.
- Investments in cryptocurrency or foreign exchange trading.



[Home](#) > [ScamSmart](#)

Be a ScamSmart investor

Avoid investment and pension scams

I want to...



Check the investment or pension opportunity to avoid scams. Go to the FCA Warning List:

www.fca.org.uk/scamsmart



**If the firm appears on this list:
the FCA has identified that they are operating without authorisation.**

Protect yourself



Business Email Compromise (BEC)

Also known as Mandate Fraud or
Payment Diversion Fraud

Criminals will:

- spend hours researching you for their scams,
- email businesses or customers,
- impersonate a company that the business has been dealing with, *and*
- request payment or inform the recipient of a change of bank account details.



**BEC can be difficult to detect;
there is no use of malware
attachments or malicious URLs.**

Protect against malware

- Beware of links and attachments in messaging.
- Prevent staff from downloading dodgy apps.
- Update your Operating System (OS), IT equipment, and apps (patching).
- Install (and turn on) antivirus software.
- Control how USB drives can be used.
- Switch on your firewall.



Backup data

Make copies of things that you value, including photos, documents, and other data stored on your IT equipment – especially in the event of a ransomware.

Make regular backups to multiple external locations and keep them somewhere physically separate:

- separate external hard drives
- thumb drive/memory stick/SD card
- cloud storage

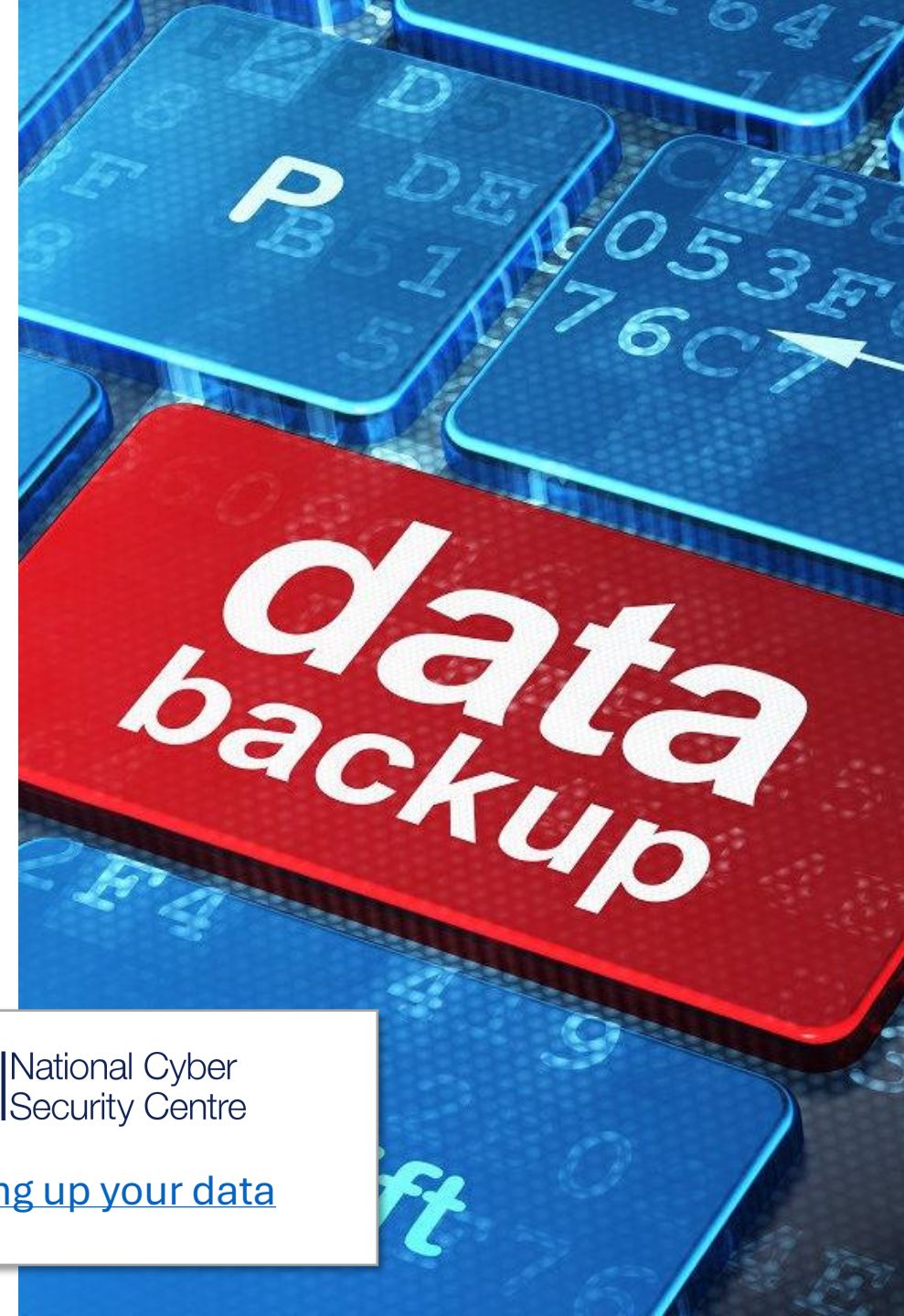


Prevention First



National Cyber
Security Centre

[Backing up your data](#)



Online presence

Are you or your staff sharing information online increasing the vulnerability of your business?

- Control what your followers need to know.
- Control who has access to the accounts.
- Use unique and strong passwords.
- Enable 2FA / 2SV or MFA.
- Google yourself/your organisation.



National Cyber
Security Centre

- [Check your cyber security](#)
- [Protect what you publish](#)



A close-up photograph of a hand using a key to unlock a door handle. The hand is positioned on the right side of the frame, with the thumb and index finger gripping the handle. The key is inserted into the lock, and the handle is being turned. The background is a blurred wooden door. The image is overlaid with a dark blue semi-transparent banner that contains the text.

Do you lock your doors?

Yes?

Do you have separate keys for all your doors?

Yes?

Then lock your online accounts with your digital key
(aka your password).

Create a strong password using 'Three Random Words'



Strength of the password:	Examples of passwords:	How long it takes for a computer to guess the password:
Very, very weak	blue	Less than a second
Very weak	waterblue	13 seconds
Weak	blueredgreen	2 minutes
A bit stronger	waterbluechair	12 hours
Strong	water!bluEchAir5	A few months/years

Turn on your **2FA** (2 Factor Authentication) or **2SV** (2 Step Verification)

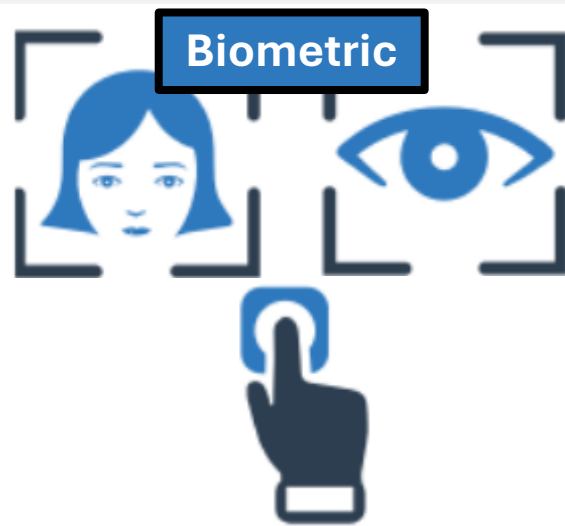
**PASSWORD
or PIN**

Something
you know



2FA

Something
you have or are



**ACCOUNT
DENIED**

If 2FA not correct,
then no access is
granted

Received notification of
access? Your password is
known - change your
password immediately.

Setting up 2-Step Verification
(2SV) - [NCSC.GOV.UK](https://www.ncsc.gov.uk)



Have your emails ever been in a data breach?

You can check using
<https://haveibeenpwned.com>



Who's Been Pwned Passwords Notify Me API Demos Pricing About ▾

Have I Been Pwned

Check if your email address is in a data breach

Using Have I Been Pwned is subject to the [terms of use](#)



HERTFORDSHIRE

CONSTABULARY

Prevention First

Tips – digital footprint



Don't click 'Unsubscribe' links blindly as it may direct you to fraudulent web pages that closely mimic legitimate unsubscribe portals.

- Do you need to handover your details for that discount or email receipt?
- Beware when using public WIFI. Are you connecting to a genuine one?
- Facebook and other social media: "People you may know". Do you know them well enough to connect / befriend them?
- Electoral Register: opt out of the Open register
- 192.com and other online telephone directories: opt out / remove yourself
- Close old and unused accounts / remove your data



Always **report** scam emails, texts, websites, adverts & phone calls

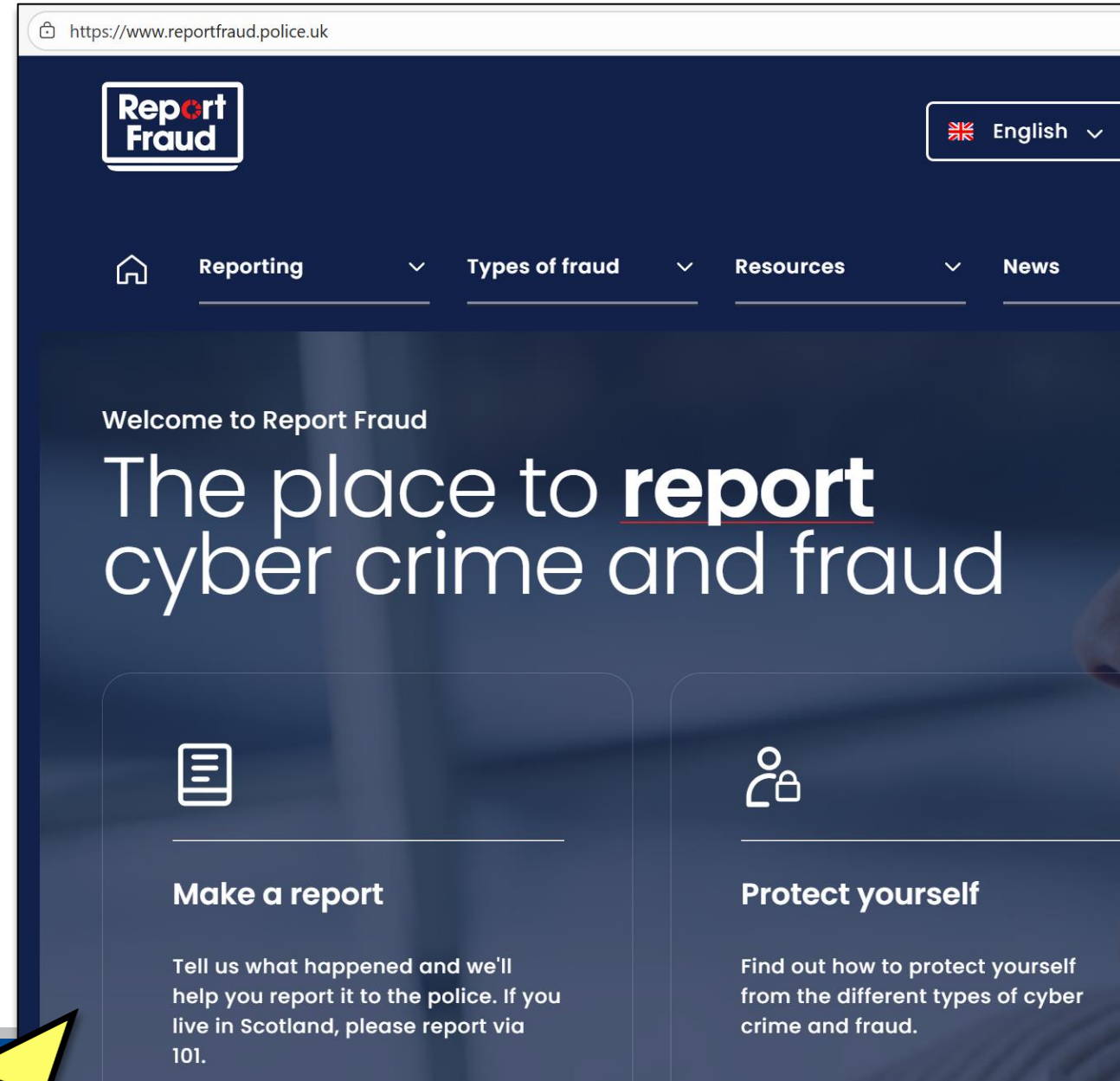
- ✓ Forward suspicious emails to report@phishing.gov.uk
- ✓ Forward scam texts to **7726** (handy tip: 7726 spells out SPAM on a phone keypad)
- ✓ **Report suspicious phone calls:** text 7726 with the word 'Call', followed by the caller's telephone number
- ✓ **Report fake/scam websites, and adverts,**
www.reportfraud.police.uk

Incurred financial loss or have been hacked as a result of responding to a phishing text message, email, phone call, social media advert or website? Report all cyber crime and fraud at www.reportfraud.police.uk or call 0300 123 2040.



If you are a victim...

1. Don't be embarrassed.
2. Scams can, and do, happen to anyone.
3. Always report to help prevent others falling victim to scams.



Herts Connected

- A free interactive messaging service from Hertfordshire Police to keep up-to-date with what is happening in your local area and crime prevention advice including events from the Police.
- Quick and easy to sign up here:
<https://www.hertsconnected.co.uk>



2026/2027 Library Events

	The below are multi-talk events: • Cyber Crime & Fraud Prevention - Herts Police • Rogue Traders & Scams - Trading Standards • Scams & Victim Support - Beacon Victim Support • Fraud against the Council - SAFS The event runs between 10.45-14.15.	The below are single talk events on Cyber Crime & Fraud Prevention by Herts Police. Check each library event for individual timings.
October	Hatfield - Wed 7th Oct 2026 Hoddesdon - Fri 16th Oct 2026	Tring - Mon 19th Oct 2026, 18.30-20.00
November	Croxley Green - Wed 4th Nov 2026	Buntingford - Tues 10th Nov 2026, 11.00-12.30
January	Hitchin - Fri 29th Jan 2027	Berkhamsted - Wed 20th Jan 2027, 10.00-11.30
February	Ware - Mon 1st Feb 2027 St Albans - Wed 10th Feb 2027	
March	Borehamwood - Wed 3rd Mar 2027	Baldock - Mon 1st Mar 2027, 10.30-12.00
April	Bishops Stortford - Thurs 29th Apr 2027	
May	Stevenage - Tues 4th May 2027	Hertford - Tues 18th May 2027, 13.00-14.30
June	Watford - Wed 9th June 2027	
July	Letchworth - Wed 14th July 2027	



Cyber and Fraud Aware?

Stay safe & secure online

All day drop-in with cyber & fraud crime prevention experts to answer your questions.

- Password & 2-step verification
- Phishing and social engineering
- Phone, email, text scams and other top tips

Coming to a library near you:

Cyber Crime & Fraud Prevention events with scheduled talks on the day. For dates and venues:

- visit www.hertfordshire.gov.uk/libraries and
- search for "cyber" in "Events and things to do at the library".







www.hertfordshire.gov.uk/libraries Further details 0300 123 4049







EasternProtect.org and Herts.police.uk/cyber-fraud
(more cyber security awareness resources)



HertsCyberProtect@herts.police.uk
(book us for more cyber security awareness sessions)



ERSOU Cyber Protect and Cyber Choices



Survey completion is appreciated



Any Questions?



[https://www.smartsurvey.co.uk/s/
HertfordshireIndividuals/](https://www.smartsurvey.co.uk/s/HertfordshireIndividuals/)