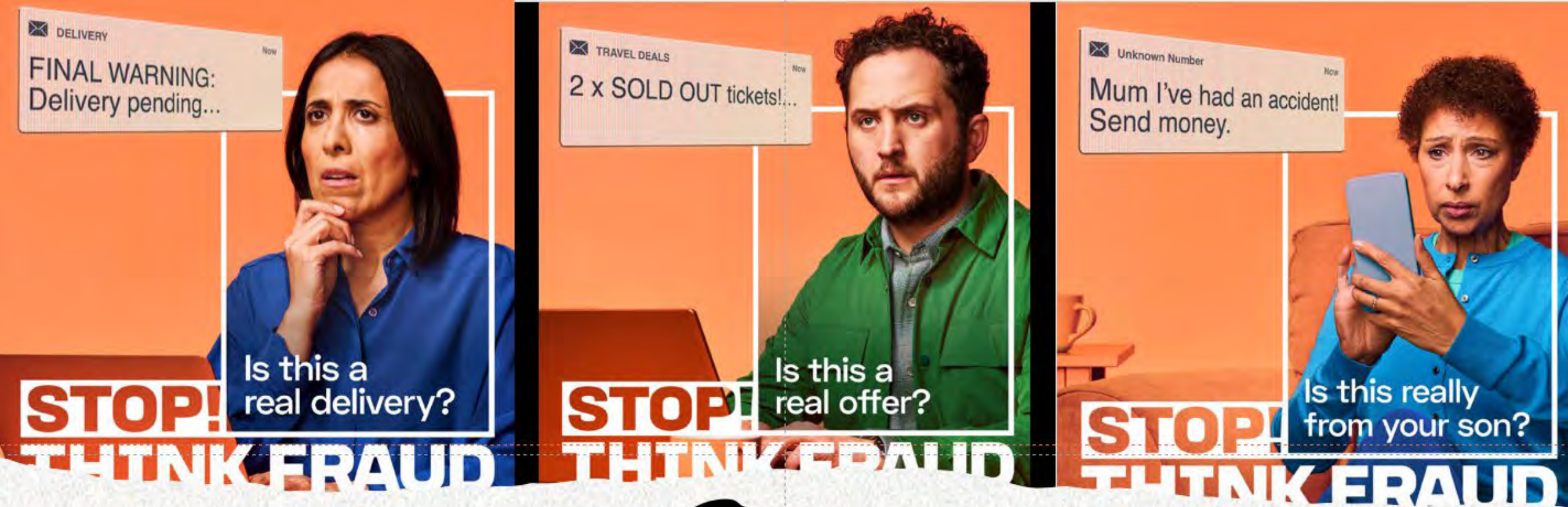


Protecting yourself from fraud & cyber crime

Chen TSUI & Alan MORDEY
Cyber Prevent & Protect Officers
Serious Fraud & Cyber Unit
Hertfordshire Constabulary

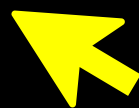
Email: hertscyberprotect@herts.police.uk





Fraud and Cybercrime accounts for 40% of reported crime

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





NO PARKING
LOW ZONE

SPYBAR

concrete

cowboy

concrete

cowboy



There is a flavour for everyone

Cyber security isn't just about technology

It's about:

1. your **privacy,**
2. your **money,**
3. your **identity,** and
4. your **safety.**



Remember **A**, **B**, **C**

A

**Accept nothing
on face value**

B

**Believe nothing
until confirmed!**

C

**CONFIRM
EVERYTHING!**



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

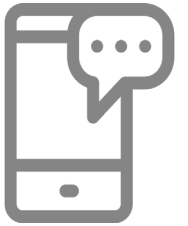
Scam messaging typically:

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
'SMSing'



phone
'Vishing'



'Quishing'

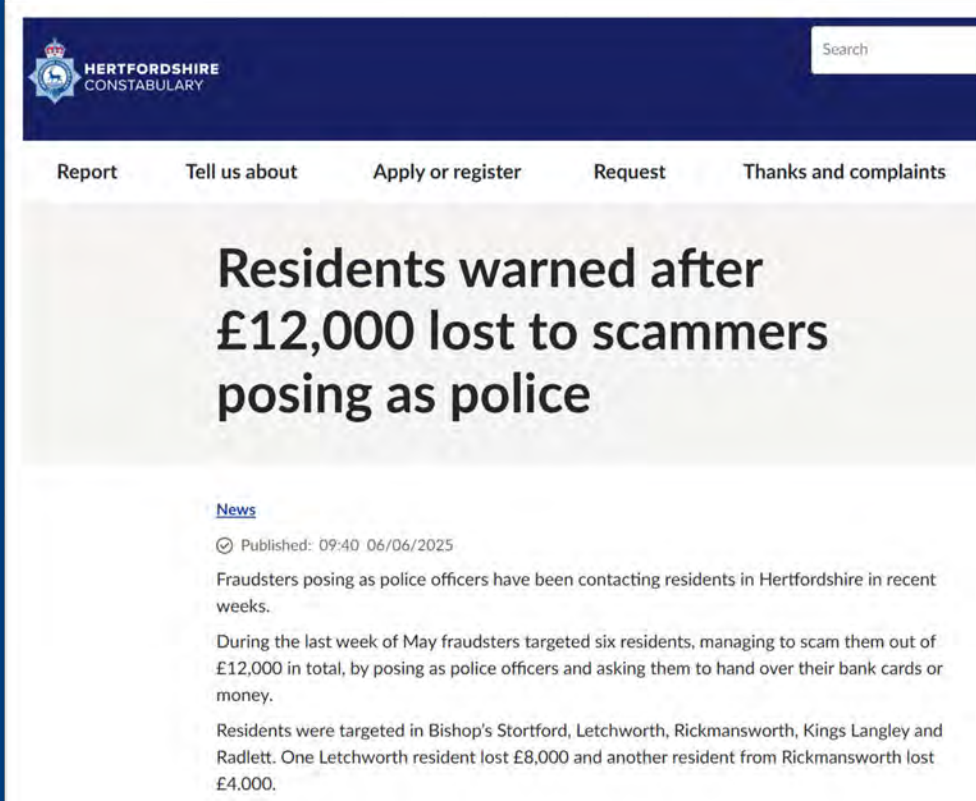


Scam Calls, Text Messages & Phishing Emails

Fraudsters 'spoof' a business' legitimate phone number or another random phone number to avoid being detected.

They claim to be:

- Your bank's fraud department, the Police, HMRC,
- Tech / computer repair support e.g. Microsoft, your internet provider,
- An investment company,
- Your mobile phone provider,
- and more...



The screenshot shows the Hertfordshire Constabulary website. The header includes the logo and name 'HERTFORDSHIRE CONSTABULARY' and a search bar. Below the header is a navigation menu with links: 'Report', 'Tell us about', 'Apply or register', 'Request', and 'Thanks and complaints'. The main content area features a news article with the headline 'Residents warned after £12,000 lost to scammers posing as police'. The article is dated 'Published: 09:40 06/06/2025' and describes how fraudsters are contacting residents in Hertfordshire, posing as police officers to steal money. It mentions that six residents were targeted in the last week of May, losing a total of £12,000. Specific locations mentioned include Bishop's Stortford, Letchworth, Rickmansworth, Kings Langley, and Radlett. One resident from Letchworth lost £8,000, and another from Rickmansworth lost £4,000.

Call from the Police...





To view the 'Rob Curling' video, please visit:
https://youtu.be/BC9P0rMy2_w?si=4UGEW-KTI4JOmG80

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:

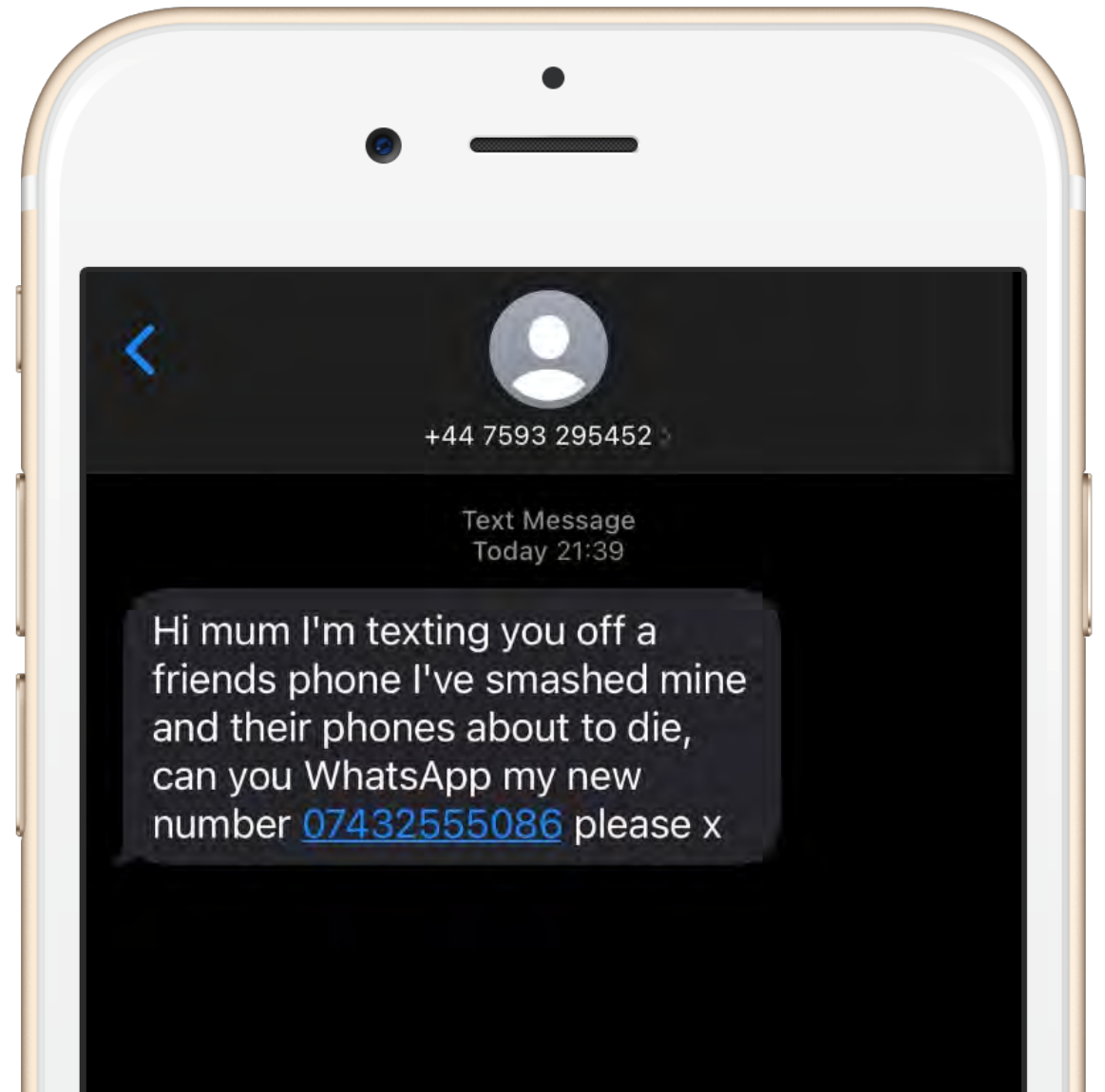
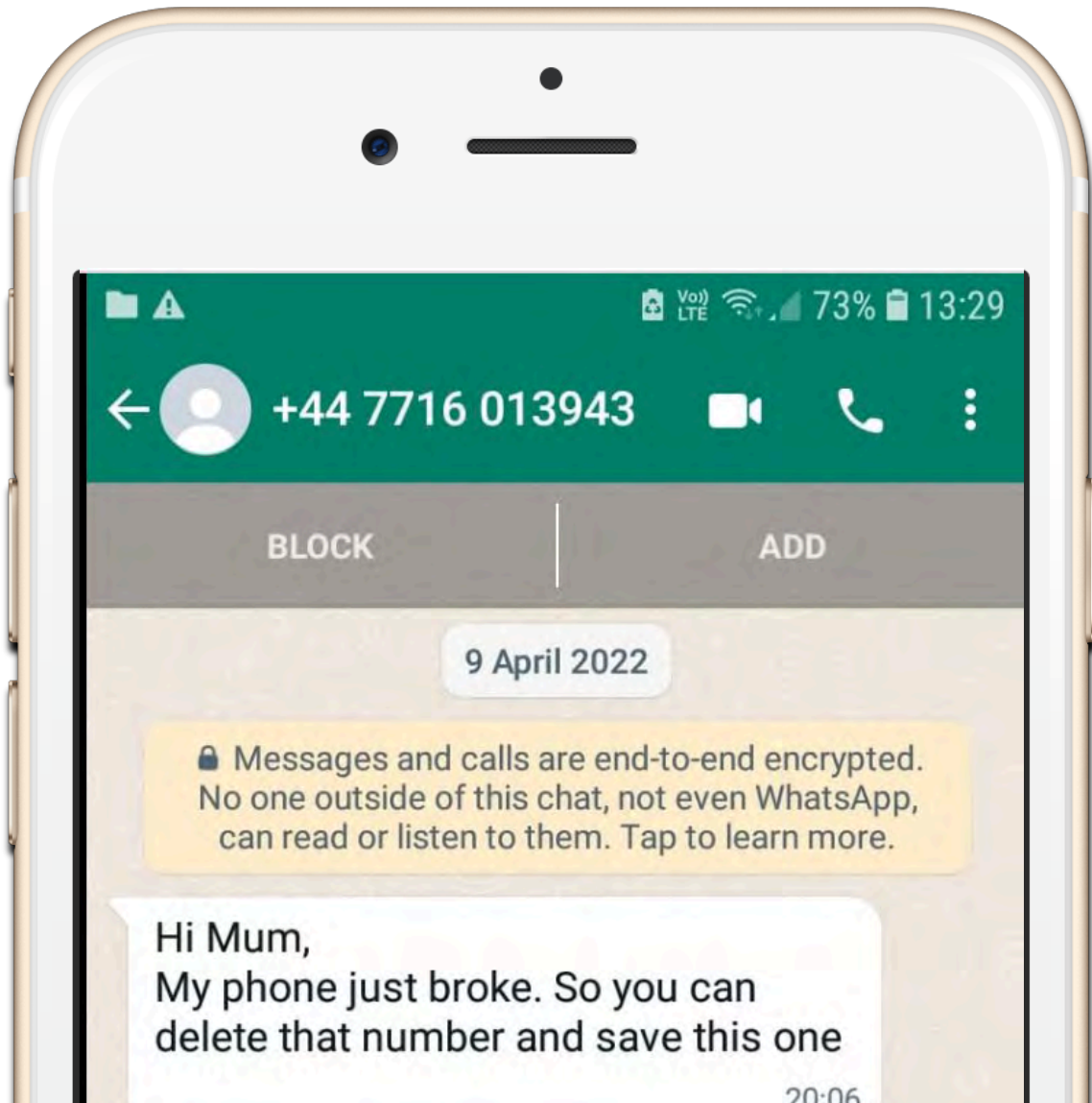
101 - to verify if the person is a police officer.

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

Hi Mum...

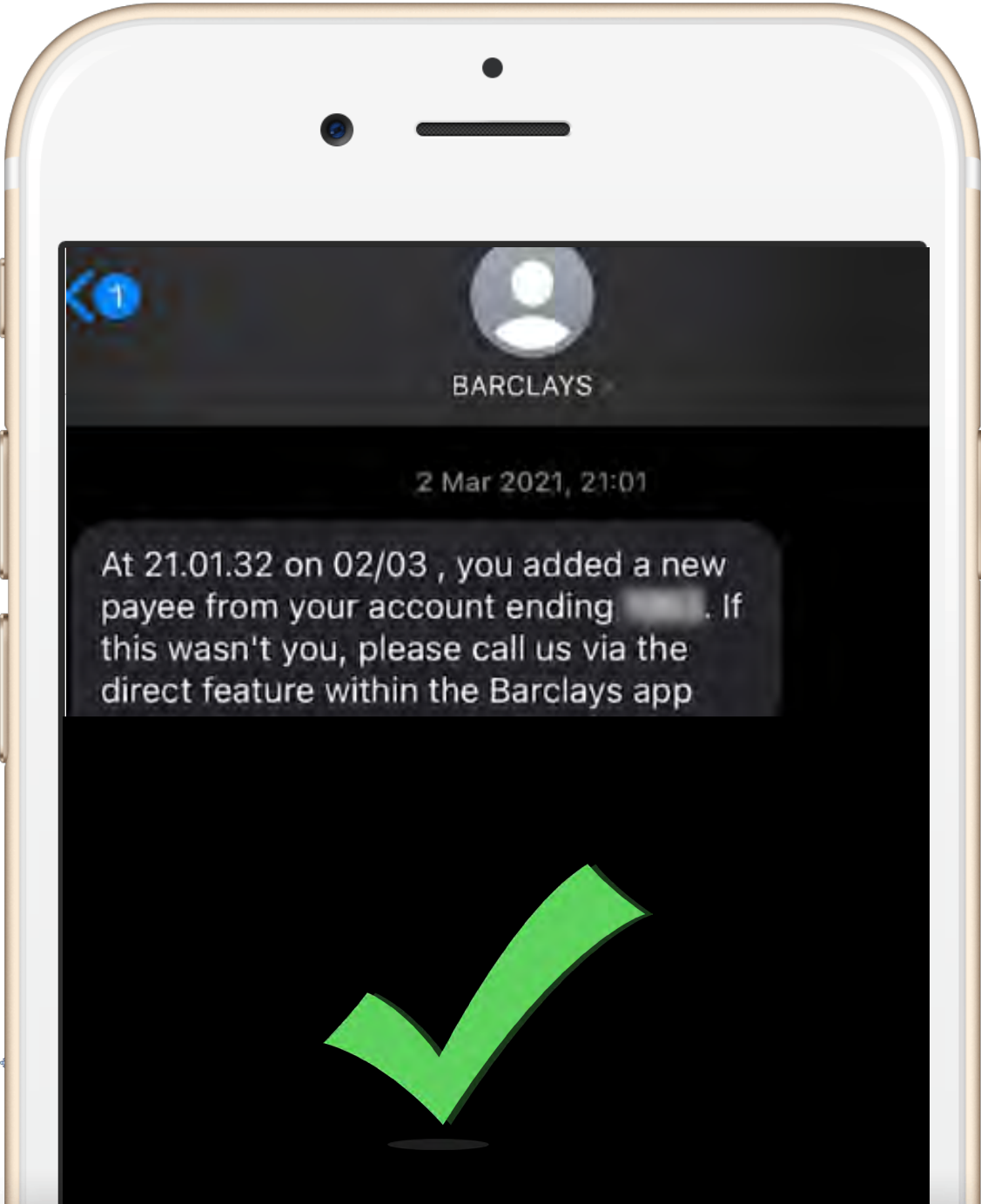


“Family/Friend in Need” Text Scam



Genuine or Fake?





Unknown number

Spelling

Fake link

<https://bar.clays-newpayee.com>

SCAM
ALERT

Check the website -


Can you spot the **fake** website! Option 1 or 2?

1. www.barclays.co.uk

2. www.barclays.co.uk



Tips:

1. Always double check the website address.
2. Never click suspicious links in messages.
3. Use the app or bookmark the website that you use often.
4. Check that the website URL begins with “http**s**” or 



Criminals keep on giving...



Phishing emails, texts, ads & signage



Reward yourself with
**TESCO Gift Card worth
up to £750!***

*PAID PARTICIPATION REQUIRED

[Get Rewarded >](#)

This message was sent automatically because your Netflix subscription has expired.

NETFLIX

Your Netflix subscription has expired!

Unfortunately, we were unable to renew your subscription. If you choose to keep your subscription active, you should update your profile.

As part of our loyalty program, you can now extend for 90 days for FREE!

[RENEW SUBSCRIPTION NOW](#)

M&

Congratu

You've been
chance to rec
Afternoon T
in with a cha
just take a moment to answer a few quick
questions about your experience.

SCAM ALERT

Hackers
Your Apple iPhone is being hacked!
Step 1: Click the button below to activate protection service by checking your Windows computer.
Step 2: You will receive a text message with a QR code to scan.
Step 3: Install the app on your iPhone.

Parking Penalty Charge Notice (PCN) issued. If you do not pay a parking fine you'll get a 'charge certificate' and you'll have 14 days to pay the fine plus 50% more. Please pay your fine by scanning the QR code at the bottom of the message.
<https://qrco.de/bfNg1q17MdpouPS>
Thank you again for your payment.
Tap to load more
08:37
Okay
RCS message

(28) Suspicious security alerts on Windows computer
We have detected that your computer is being accessed from an unusual location and improper session handling.
Your IP address:
Internet Provider: M247
Risk Score: HIGH
Time
How to resolve this
Step 1: Click the button below to activate protection service by checking your Windows computer.
Step 2: Activate the protection service by scanning the QR code at the bottom of the message to keep your computer active.
PROTECT YOURSELF

11:20
DWP: As the Winter payment is complete, you will receive a receipt of the application. I
Hemisphere
a cold spell
allowance
released. You
a tax-free
between £2
Please complete
application
12 deadline
<https://qrco.de/bfNg1q17MdpouPS>
<https://qrco.de/bfNg1q17MdpouPS>
G6pzZkio
The Winter
payment is
complete
within one
receipt of the application. I

07463 265589 created this group
Yesterday
07463 265589
Tik Tok
Daily income: £300-800
• No experience required
• No time or location restrictions
• You only need a mobile phone to operate
Please click the link below to claim a **£8** bonus!
This chat is now end-to-end encrypted
RCS message

Enfield Council · Follow
19h ·
We're issuing a warning to our residents who park their vehicles in the borough. Our teams have discovered and removed a fake QR code from pay-to-park signage.
You will not be asked to scan a QR code to pay for parking. You should pay with the PayByPhone App, by calling 0330 400 7275 or at local shops displaying the PayPoint sign.
Also, we never issue parking fines, known as PCNs, by text. If you get a demand for payment by text, ignore and delete the message.
Find out more about reporting fraud at Stop Think Fraud here: <https://orlo.uk/FNmiV> #SaferEnfield



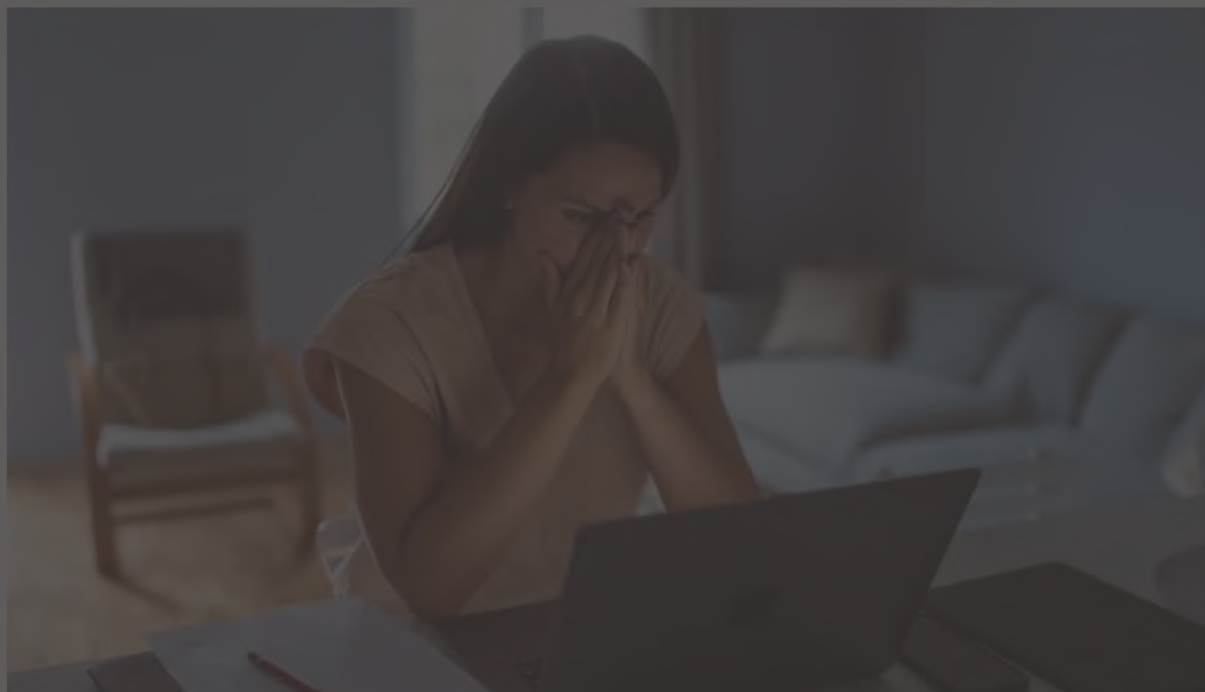
Necessary adjustments to follow

NEWS

Home | InDepth | Israel-Gaza war | US election | Cost of Living | War in Ukraine

Business | Market Data | Economy | Technology of Business | AI Business

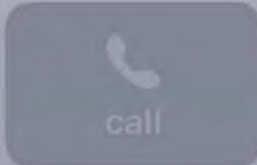
Banks must refund fraud up to £85,000 in five days



Done



The Co-operative



other

wannee.may@obecmail.org

The Banking Team

'Phishing' emails



[Account-Deactivation]



Microsoft Fix <mx-59545445435@protection.office-365.com>

Tuesday, August 21, 2018 at 1:18 AM
[Show Details](#)

Office-365

Hi Sales

Your account of [redacted] .com will be disconnected from sending or receiving mails from other users. because you failed to resolve errors on your mail.

You need to resolve the errors or your account will be disconnected from [redacted] .com.
Follow the instruction below to resolve now.

[RESOLVE ISSUE NOW](#)

Regards,
Microsft Security Team

This notification was sent to [redacted] .com of Microsoft.com.

Sign in to your account



accountoffice.dynv6.net/

https://

Microsoft

Sign in

Email, phone, or Skype

No account? [Create one!](#)

[Can't access your account?](#)

Great offers on social media & websites





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 📌



Too good
to be true...

... and it
usually is!

Scam ads & websites

 **Wetherspoons**
13 July at 02:57 · 🌟

Hello everyone! I'm Tim Martin, for introduce you to my son Ryan Ma all control to my eldest Son. Before thanks because without all of your shares&comments within the next be used for Breakfast, lunch or dinner



Dear Customer, Due to the closure of our physical stores, to facilitate inventory clearance at these locations, we are offering an 80% online promotional discount. This week only. All inventory must go! Quantities are limited. Get it now before it's out of stock!



DDIXV.TOP
Direct clearance from the store, discount up to 80%

Shop now

 **Louisa's Tips**
Sponsored · 🌐

Enter your
DOB and we'll



Just press the LIKE



FREE DINNER FOR TWO




Harvester



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.



About the ad

Multiple versions of this ad ⓘ

< 1 of 2 >


 **UK Bonds Investments**
Sponsored ⋮
ID: 261812169252413

£50,000 Minimum Investment - Fixed Rate, Fixed Return, 1-5 Year Options, Monthly Interest Paid To Your Bank Account



About the Page

[See ads](#)

 **UK Bonds Investments**
@ukbondsinvestments
0 likes · Investment management company

More info


Bonds are Fully Guaranteed Fixed Returns Available 1-5 Year
Terms FCA Regulated Monthly Interest Paid





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.**

Deep Fakes, Misinformation & Disinformation





Steve Youell
about a week ago



facebook


ricane Helene.
is tragically.

donation or go

VERDICT: False

I don't think I want this picture on FB. They have been deleting it.

3.7K 71 166K

A woman with dark hair pulled back, wearing a white long-sleeved shirt, dark blue jeans, and light-colored sneakers, is sitting on a white modern-style chair. She is looking directly at the camera with a neutral expression. The background is a dark, almost black studio space with some faint equipment visible on the left and right sides.

To view 'Without Consent' video, please visit:
https://www.youtube.com/watch?v=F4WZ_k0vUDM&t=3s

Protect yourself





Lock your doors!

Which of these passwords is the strongest?

1. **Qwerty123** - Commonly used password!
2. **Pa55w0rd** - Commonly used password!
3. **EpicCamelMountain35%**
4. **oe4D!3£** - Not enough characters and how will you remember 20, 30, 40+ unique passwords like this?



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



**Edward Snowden on passwords:
Margaretthatcheris110%SEXY**

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

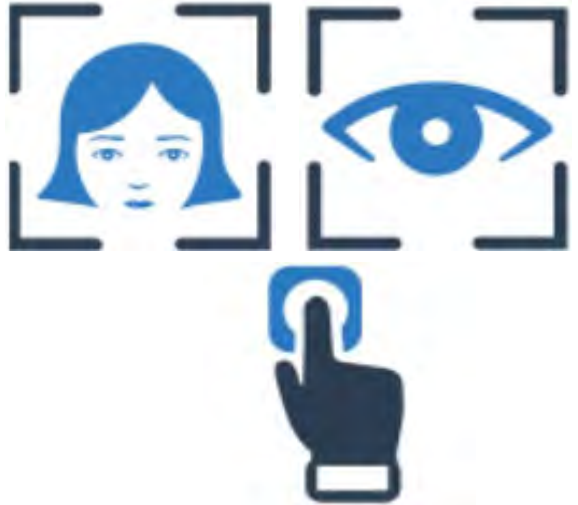
PASSWORD
or PIN

Something
you know



2FA

Something
you have or are



ACCOUNT
ACCESS

If both correct,
then access is
granted



Back up your data

In case:

- **Your device is lost, stolen or broken.**
- **Accidentally deleted data (or becomes unreadable).**
- **Your account/device is infected because of a virus.**



Update your devices

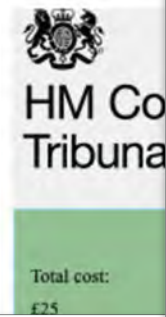
- Phones, tablets and computers.
- Smart devices (Ring doorbells, smart watches, etc).
- If possible, avoid buying and using phones that are no longer supported by the manufacturer.

Note: Windows 10 devices is **unsupported** from 14th October 2025!



Watch out for MalWare (Malicious Software)

- attachments shared by email (e.g viruses and other harmful software that can compromise your device),
- or
- links in emails that can go to malicious websites that are disguised as genuine websites.



Potentially Dangerous Viruses Detected

Dear User,

Important Notice:

Your Device May Be at Risk

Our advanced security system has identified significant threats on your device that could expose your personal information, privacy, and financial data to potential risk.

Please take a moment to review these details to understand the severity of the threats detected:

Virus Name	Potential Impact
Trojan.Win32.Generic	Steals personal information and bank details
Worm.P2P.Palevo	Spreads through network and corrupts files
Backdoor.Bot	Allows remote control of your device
Spyware.Win32.Agent	Monitors browsing activity and steals data

To fully remove these threats and secure your data, activate our recommended antivirus protection immediately. This is the only effective solution to stop further infection and safeguard your information.

[Activate Protection Now](#)

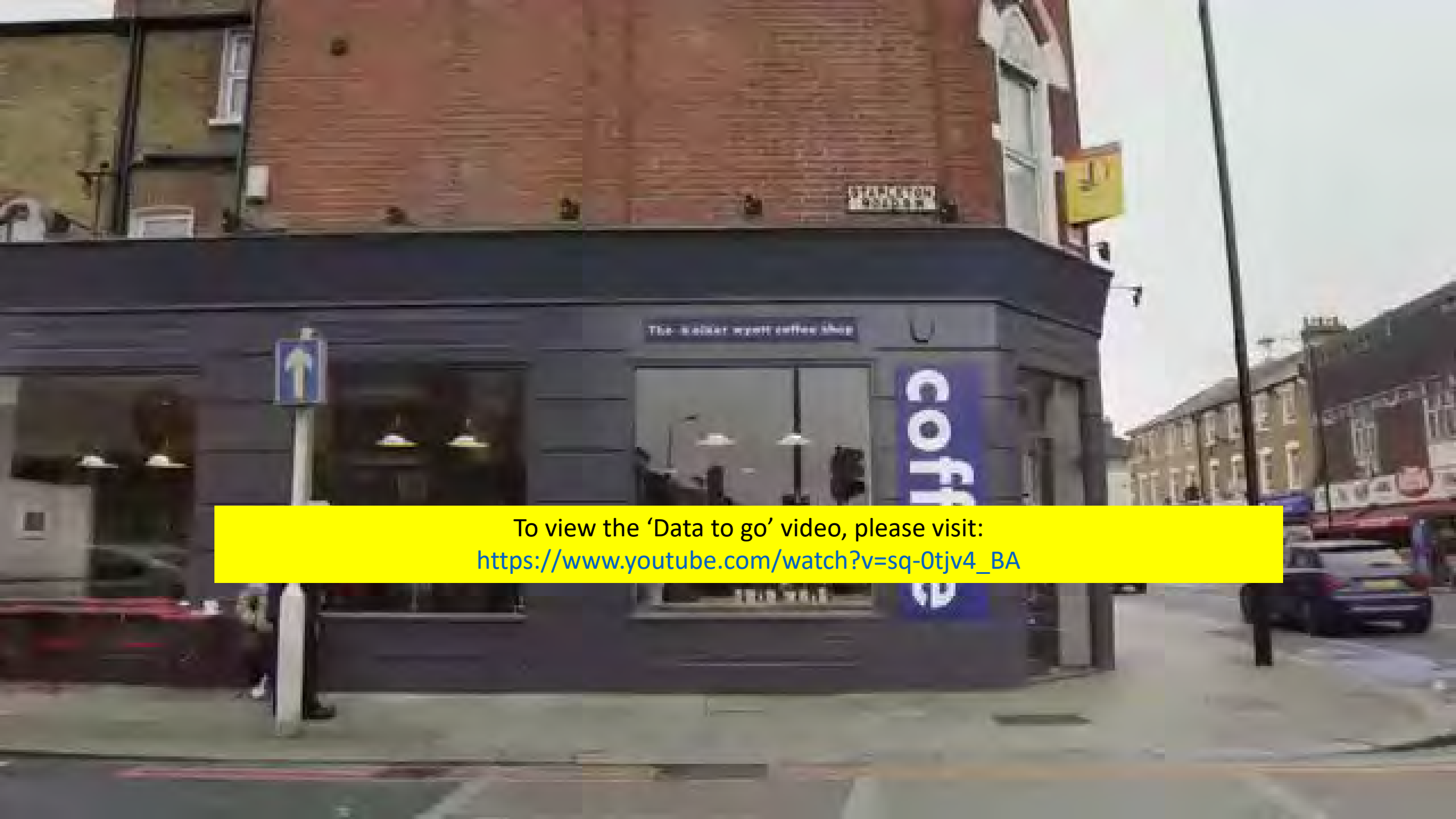
If you need assistance or have questions, please contact our support team at support@example.com

[Unsubscribe](#)

Your digital footprint

Any activity conducted across the internet leaves a trace or 'digital footprint'.



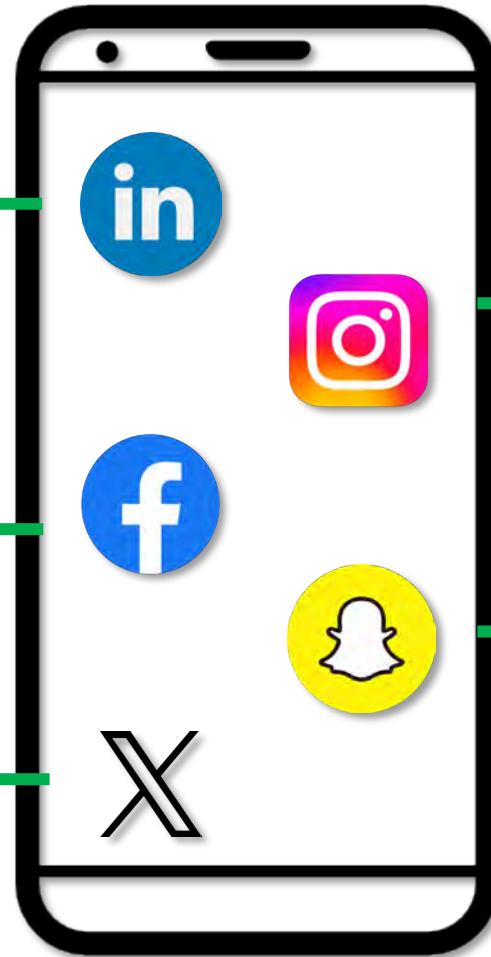


To view the 'Data to go' video, please visit:
https://www.youtube.com/watch?v=sq-0tjv4_BA

Tips for Social Media

- ✓ Enable 2SV/2FA
- ✓ Turn off activity broadcasts
- ✓ Check who can see your connections

- ✓ Review profile “about” settings – education, work, relationships, family, life events etc.
- ✓ Limit past posts
- ✓ Check who can see your friends and followers
- ✓ Check who can view your photos



- ✓ Make account private
- ✓ Disable activity status and location

- ✓ Turn on “ghost mode” to hide your location
- ✓ Disable quick-add
- ✓ Stop sending data usage

Tips – digital footprint

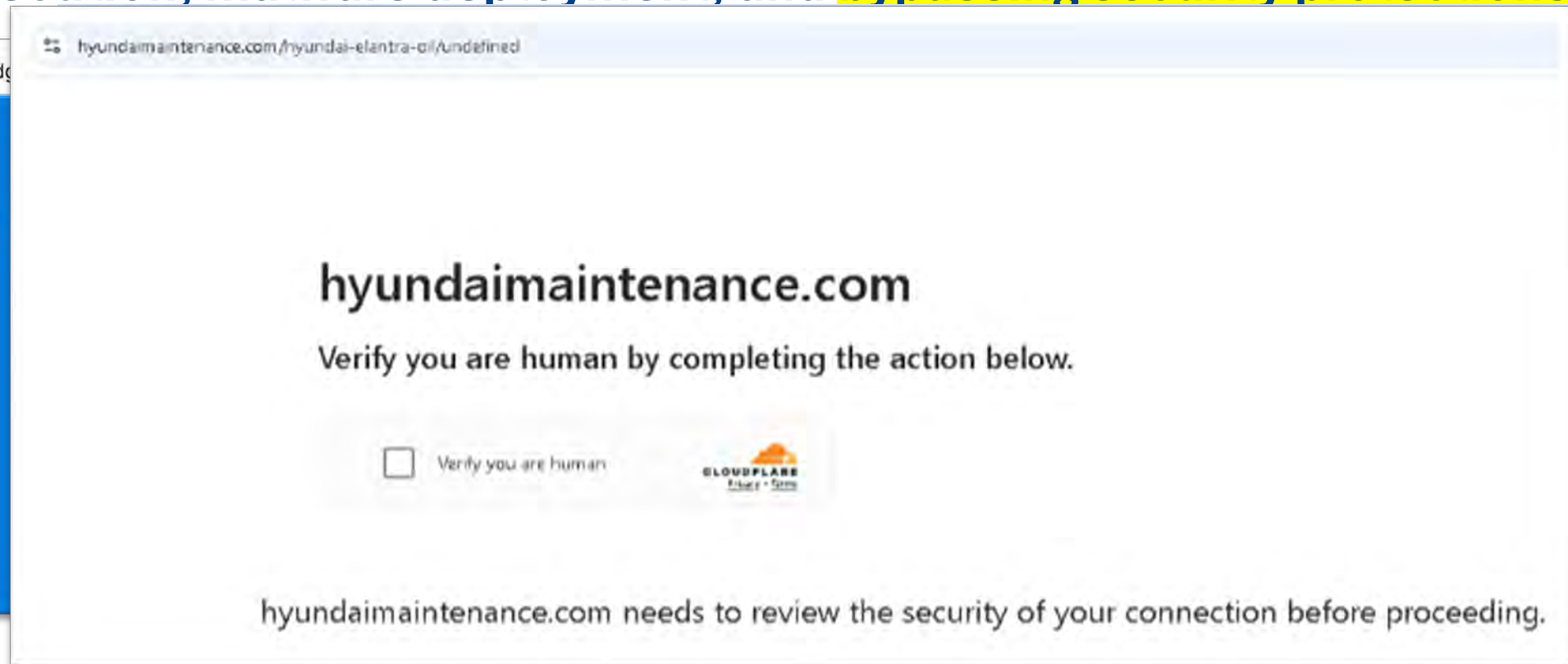
- Do you need to connect your smart device to the internet?
- Do you need to handover your details for that discount or email receipt?
- Beware when using public WIFI. Are you connecting to a genuine one?
- Facebook and other social media: “People you may know”. Do you need to connect / befriend?
- Electoral Register: opt out of the Open register
- 192.com and other online telephone directories: opt out / remove yourself

Close old and unused accounts – they all have your data!



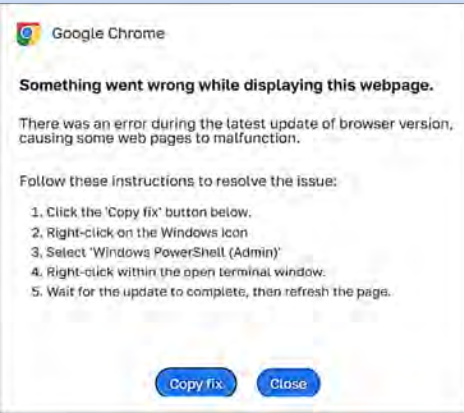
Beware of ClickFix techniques

ClickFix (aka FileFix, ConsentFix, ClearFix) is a social engineering that uses a fake error or verification message to manipulate victims into **copying and pasting a malicious script** and then running it – leading to remote code execution, malware deployment, and **bypassing security protections**.

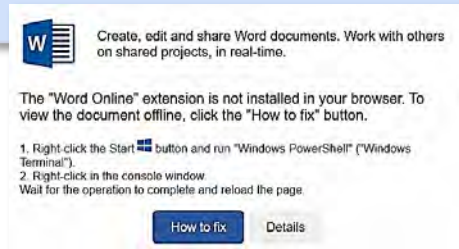


ClickFix techniques

Unable to display the web page; you need to install a browser update.



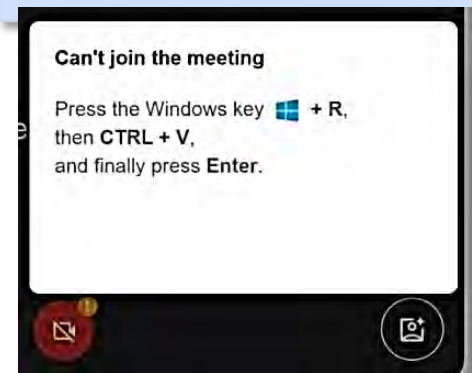
Error loading a Word or PDF document on a website or from an email. You see a .pdf or .docx icon, but in reality the file opens in a web browser and asks you to install a plugin.



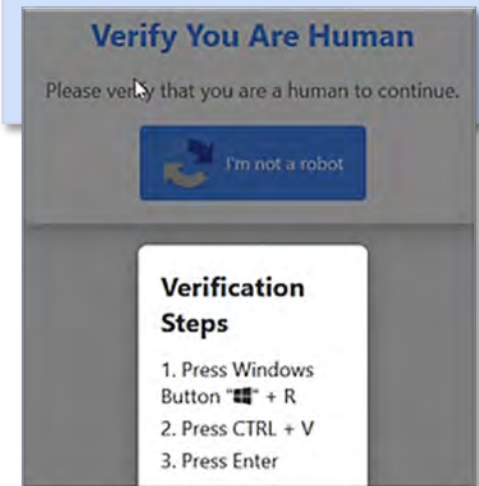
Sponsored listings (ads) in web searches e.g. searches for ChatGPT Atlas Browser in Google.



Issues with your microphone and camera in Google Meet or Zoom. You receive a link for a video call, but 'you are not allowed to join', because there are problems with the microphone and camera. The message explains 'how to fix it'.

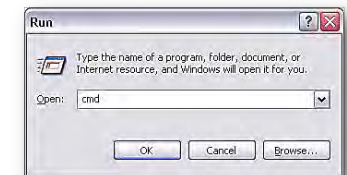
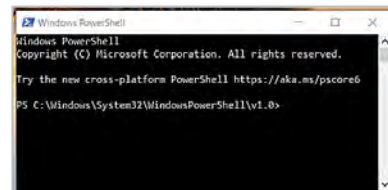


Prove that you're not a robot – fake CAPTCHA. You are required to follow the instructions written in the pop-up window.



How to protect yourself (and your organisation) from ClickFix attacks?

- ✗ Don't click on sponsored search results (sponsored ads).
- ✗ Never copy and paste text from a web page into a computer's Run box or File Explorer



Report
fraud & cyber crime!



Call 0300 123 2040
reportfraud.police.uk



Action Fraud has now been replaced with Report Fraud

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

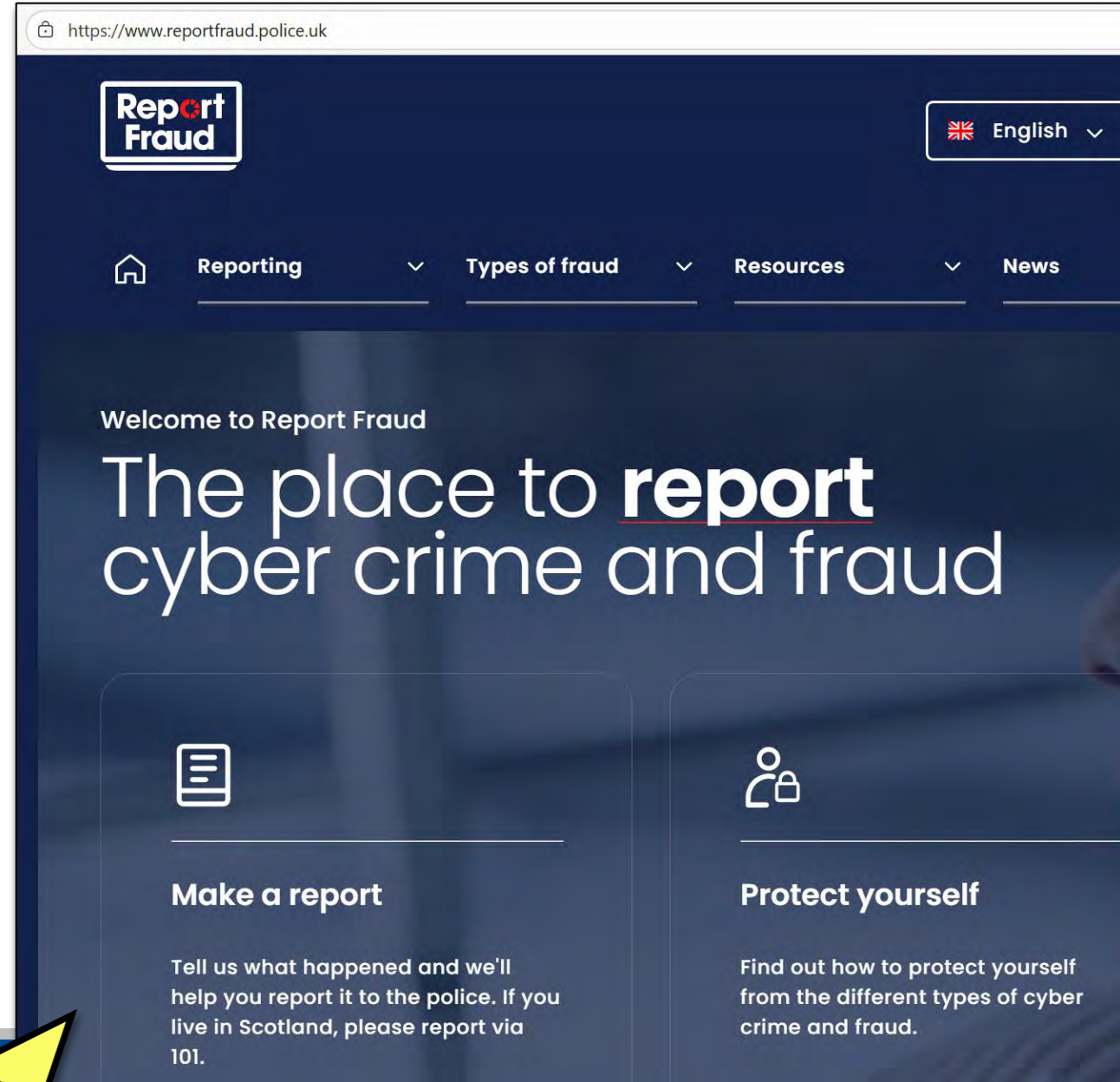
- ✓ Forward suspicious emails to report@phishing.gov.uk
- ✓ Forward scam texts to **7726** (handy tip: 7726 spells out SPAM on a phone keypad)
- ✓ Report suspicious phone calls: text 7726 with the word 'Call', followed by the caller's telephone number
- ✓ Report fake/scam websites, and adverts, www.reportfraud.police.uk

Incurring 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...

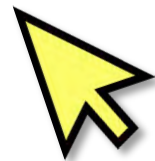
1. Don't be embarrassed.
2. Scams can, and do, happen to anyone.
3. Always report to help prevent others falling victim to scams.



The screenshot shows the homepage of the Report Fraud website. At the top, there is a navigation bar with the 'Report Fraud' logo on the left and a language selector set to 'English' on the right. Below the navigation bar, there are four main menu items: 'Reporting', 'Types of fraud', 'Resources', and 'News', each with a dropdown arrow. The main content area features a large heading: 'Welcome to Report Fraud' followed by 'The place to report cyber crime and fraud'. Below this, there are two prominent call-to-action boxes. The first box, titled 'Make a report', includes a document icon and text stating: 'Tell us what happened and we'll help you report it to the police. If you live in Scotland, please report via 101.' The second box, titled 'Protect yourself', includes a person icon and text stating: 'Find out how to protect yourself from the different types of cyber crime and fraud.' A yellow mouse cursor is pointing at the bottom right corner of the screenshot.

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>



The screenshot shows the homepage of the Herts Connected website. At the top left is the 'Herts Connected' logo, which consists of a speech bubble icon and the text 'Herts Connected'. To its right is the Hertfordshire Constabulary crest and the text 'HERTFORDSHIRE CONSTABULARY'. Below the header is a large photograph of three police officers in uniform kneeling on a grassy area. They are positioned around a white van with blue and yellow checkered stripes, labeled 'DOG UNIT'. Two police cars with similar checkered stripes are parked on either side of the van. A 'Menu' icon is visible in the top right corner of the page. Below the photograph, the text reads 'Welcome to Herts Connected' followed by the subtext 'Get connected with what is happening in your local area, keep up to date and have your say in what goes on where you live or work in Hertfordshire'.

Cyber crime & fraud awareness events in a library near you:

- Hoddesdon - Fri 30 Jan 2026
- St Albans - Wed 4 Feb 2026
- Hitchin - Fri 27 February 2026
- Borehamwood - Wed 11 March 2026
- Hatfield - Fri 20 March 2026
- Bishops Stortford - Wed 15 Apr 2026
- Ware - Mon 20 Apr 2026
- Watford - Wed 3 June 2026
- Stevenage - Mon 8 June 2026
- Rickmansworth - Fri 3 July 2026



Cyber and Fraud Aware?

Stay safe & secure online

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

FREE event
No tickets or booking required

Coming to a library near you:

Cybercrime & 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".

A yellow arrow points from the bottom left of the poster towards the event list.



**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/)