rocu south east
Regional Organised Crime Unit

National Cyber Security Centre
a part of GCHQ

Cyber Aware

How to stay secure online

cyberaware.gov.uk

For: Bagshot Society on the behalf of Surrey and Sussex Police Cyber Protect Team
On: 21st March 2023
Summary notes

Delivered by: Mr Mark Godsland CISMP
TVP/SEROCU: Police Cyber Security Advisor

This information is exempt under the freedom of Information Act 2000(FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to **ncscinfoleg@ncsc.gov.uk.**

All material is UK Crown copyright ©.

Summary of what to expect in the coming slides

A 'High Level' over view of the current, risks from the perspective of the wider community. (Individuals) All content is taken from the National Cyber Security Centre or NFIB/ NCA / CoLP/ ICO / Ofcom

Traditional Fraud types for those not digitally connected

Affect of online Fraud in the UK

Cyber Aware, looking at their top tips to protect yourselves and stay secure online

Phishing (Examples of current COVID-19, Vaccination Scams and other scams)

Reporting of suspicious websites, emails & text messages

Data Breaches

Safe use of social media

Smart devices

Online shopping

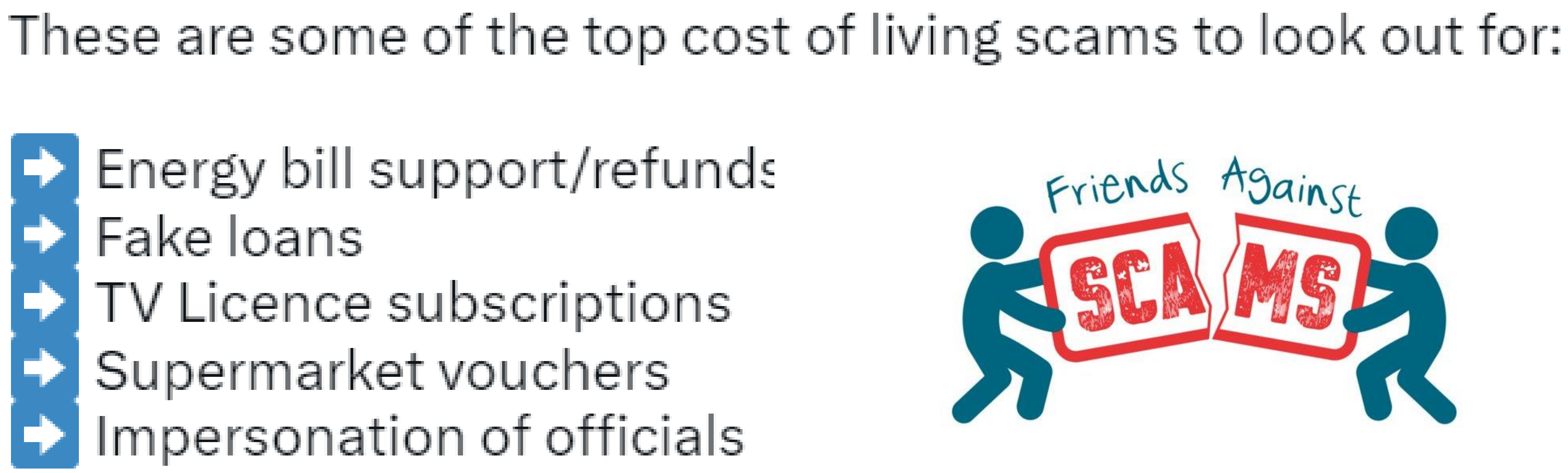
How and where to report Fraud / Cyber Crime

Summary and signposting to further advice, guidance and information.

Note. All content correct as of of 16th March 2023

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk.
All material is UK Crown Copyright © CITY OF LONDON POLICE: SUITABLE FOR PUBLICATION

Traditional Fraud methods

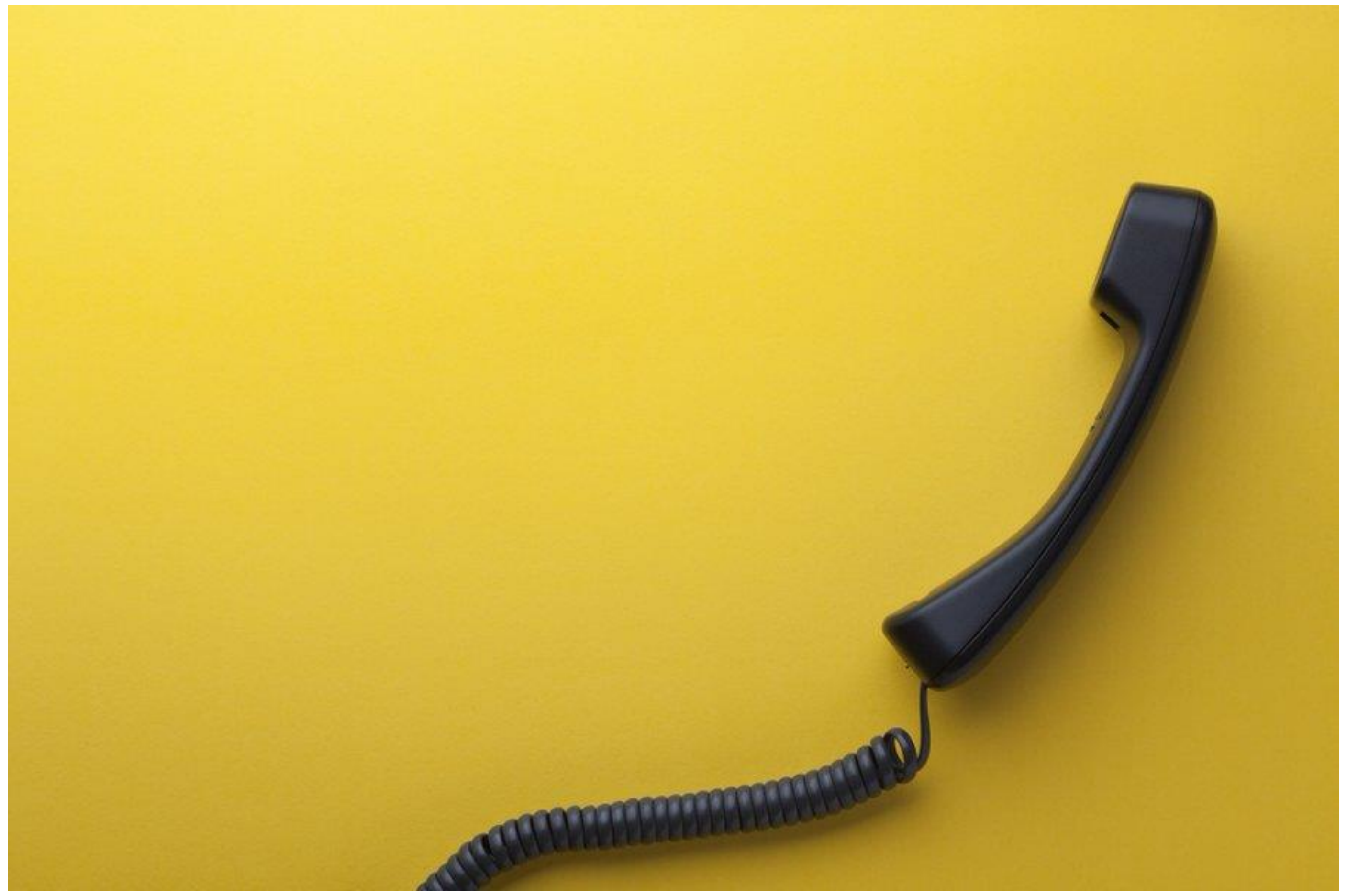


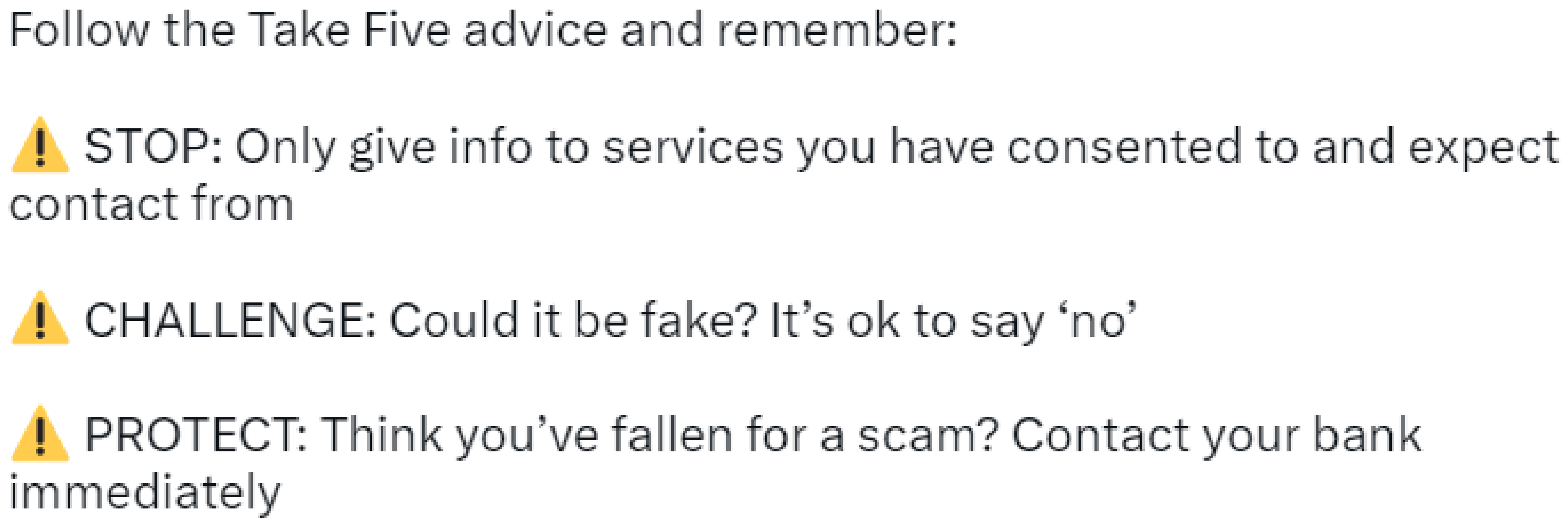
These are some of the top cost of living scams to look out for:

- ➡ Energy bill support/refunds
- ➡ Fake loans
- ➡ TV Licence subscriptions
- ➡ Supermarket vouchers
- ➡ Impersonation of officials

Friends Against SCAMS

Always verify unsolicited calls, texts, emails and letters via a trusted method





Follow the Take Five advice and remember:

⚠️ STOP: Only give info to services you have consented to and expect contact from

⚠️ CHALLENGE: Could it be fake? It's ok to say 'no'

⚠️ PROTECT: Think you've fallen for a scam? Contact your bank immediately

[Friends Against Scams - National Trading Standards (NTS) Scams Team initiative protecting and preventing people from becoming victims of scams]

ACTION REQUIRED

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk.
All material is UK Crown Copyright © CITY OF LONDON POLICE: SUITABLE FOR PUBLICATION

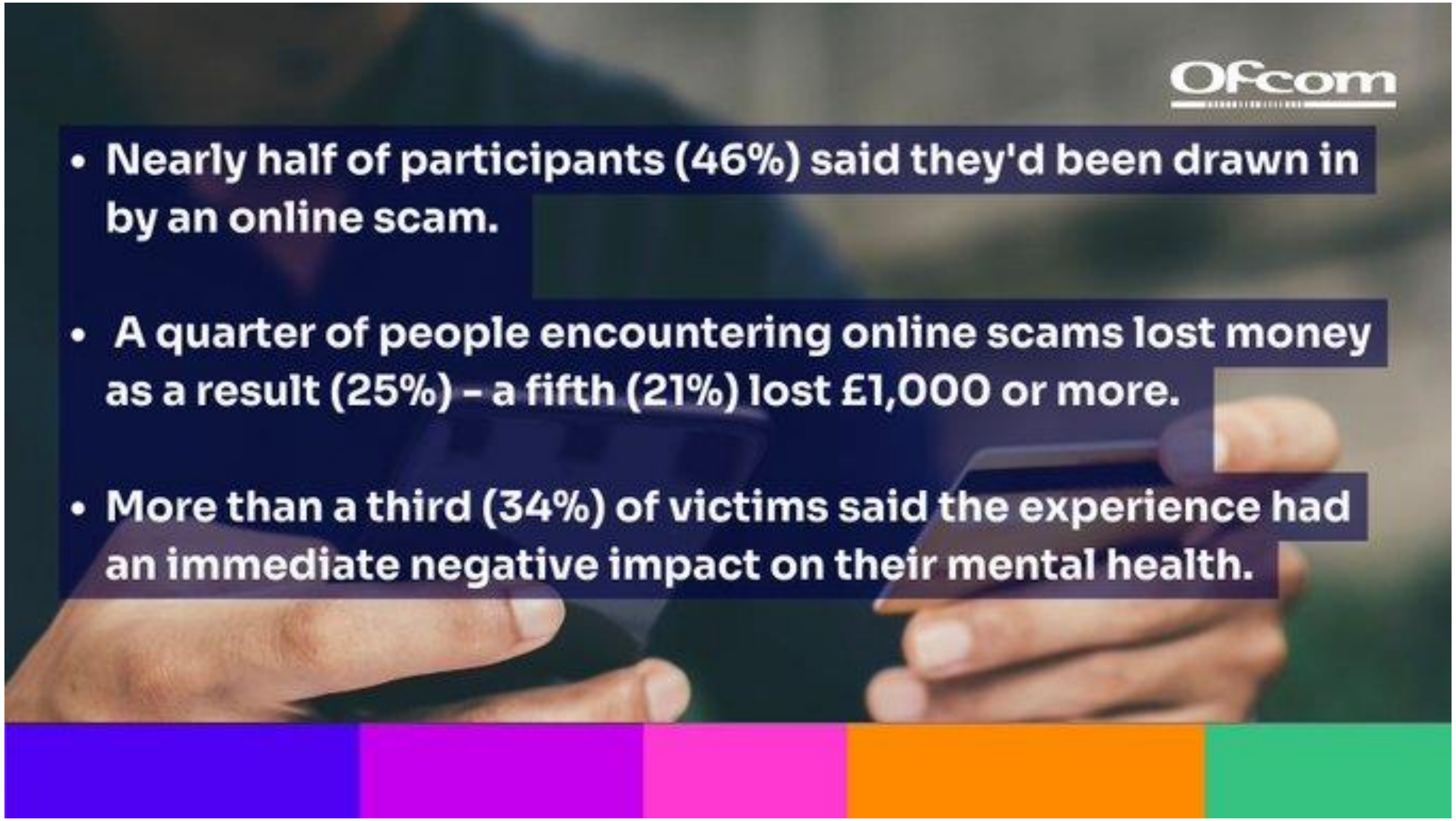
Scale and impact of online fraud revealed

News | Online safety

National Cyber Security Centre
a part of GCHQ

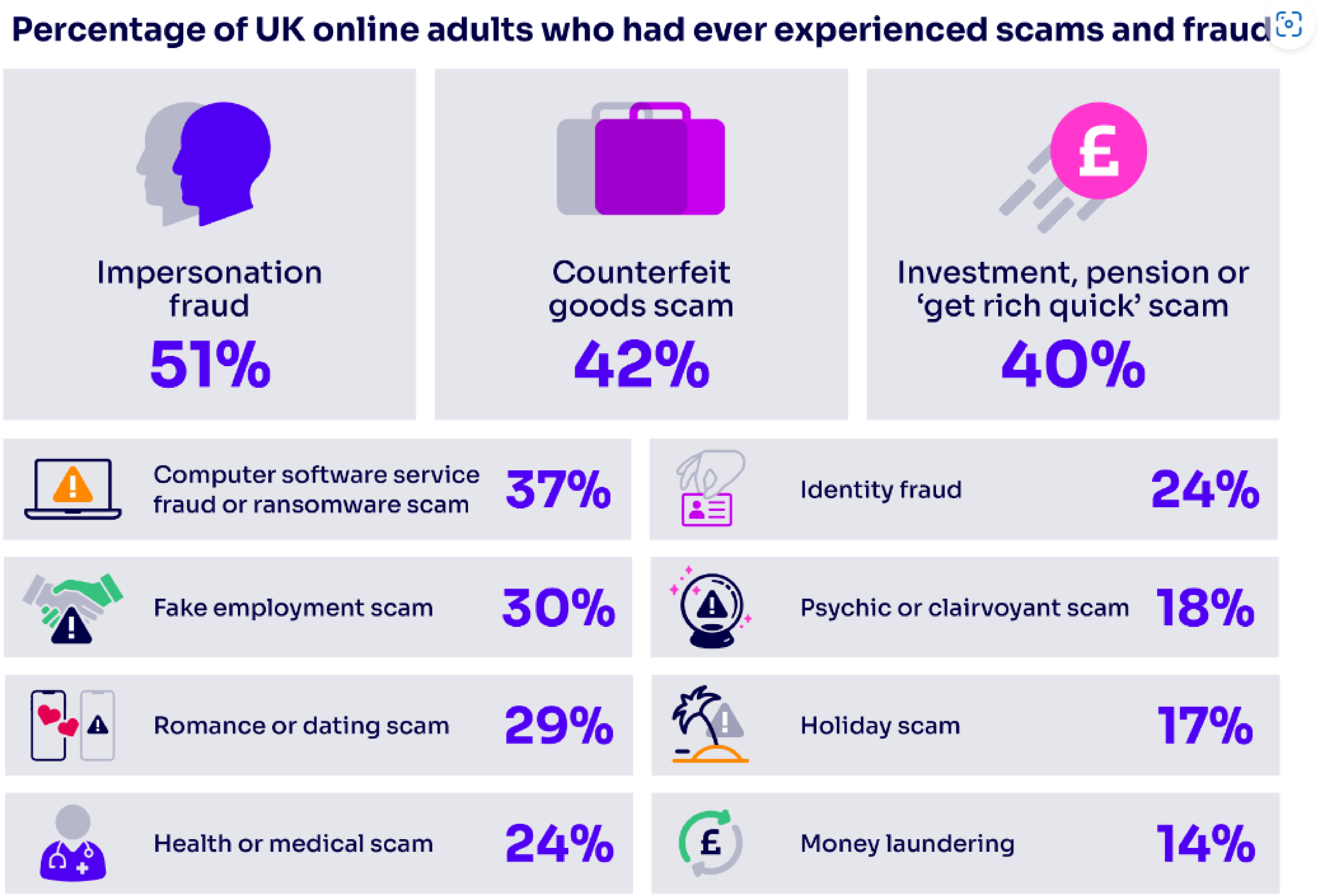
Cyber Aware

Source Ofcom 16th March 2023



- Nearly half of participants (46%) said they'd been drawn in by an online scam.
- A quarter of people encountering online scams lost money as a result (25%) – a fifth (21%) lost £1,000 or more.
- More than a third (34%) of victims said the experience had an immediate negative impact on their mental health.

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk.
All material is UK Crown Copyright © CITY OF LONDON POLICE: SUITABLE FOR PUBLICATION



Percentage of UK online adults who had ever experienced scams and fraud

Impersonation fraud	51%
Counterfeit goods scam	42%
Investment, pension or 'get rich quick' scam	40%
Computer software service fraud or ransomware scam	37%
Identity fraud	24%
Fake employment scam	30%
Psychic or clairvoyant scam	18%
Romance or dating scam	29%
Holiday scam	17%
Health or medical scam	24%
Money laundering	14%

https://www.ofcom.org.uk/news-centre/2023/scale-and-impact-of-online-fraud-revealed?utm_source=tw_graphic&utm_medium=social_org&utm_campaign=onlinesafety23

ACTION REQUIRED

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk.
All material is UK Crown Copyright © CITY OF LONDON POLICE: SUITABLE FOR PUBLICATION

National Cyber Security Centre
a part of GCHQ
Cyber Aware

Cyber Aware and staying secure online

From banking to shopping, and streaming to social media, people are spending more time than ever online. Cyber Aware is the government's advice on how to stay secure online.

Cyber Aware led by the National Cyber Security Centre (NCSC) and delivered in partnership with the Cabinet Office, Home Office and the Department for Digital, Culture, Media & Sport.

Designed to empower and enable the public to better understand how to stay secure online and to take practical steps to help do so.

This focus’s on Cyber Security

What is cyber security?
Cyber security is the means by which individuals and organisations reduce the risk of being affected by cyber crime.

Cyber security's core function is to protect the **devices** we all use (smartphones, laptops, tablets and computers), and the **services** we access online - both at home and work - from theft or damage.

It's also about preventing unauthorised access to the vast amounts of **personal information** we store on these devices, and online.

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk.
All material is UK Crown Copyright © CITY OF LONDON POLICE: SUITABLE FOR PUBLICATION

Cyber Aware https://www.ncsc.gov.uk/cyberaware/home

National Cyber Security Centre
a part of GCHQ
Cyber Aware

Take your email security to another level
Your email is where you keep your most personal and financial information.

If a hacker accesses your email, they could access your other online accounts using the 'forgot password' feature (which often sends you an email) access personal or business information and use this to scam you or people you know.

This guide outlines the Cyber Aware top tips and advice on how to:

- Protect your **accounts (How to guides are listed in each of the tips, via web links in blue)**
- Protect your **devices** and **data / information**

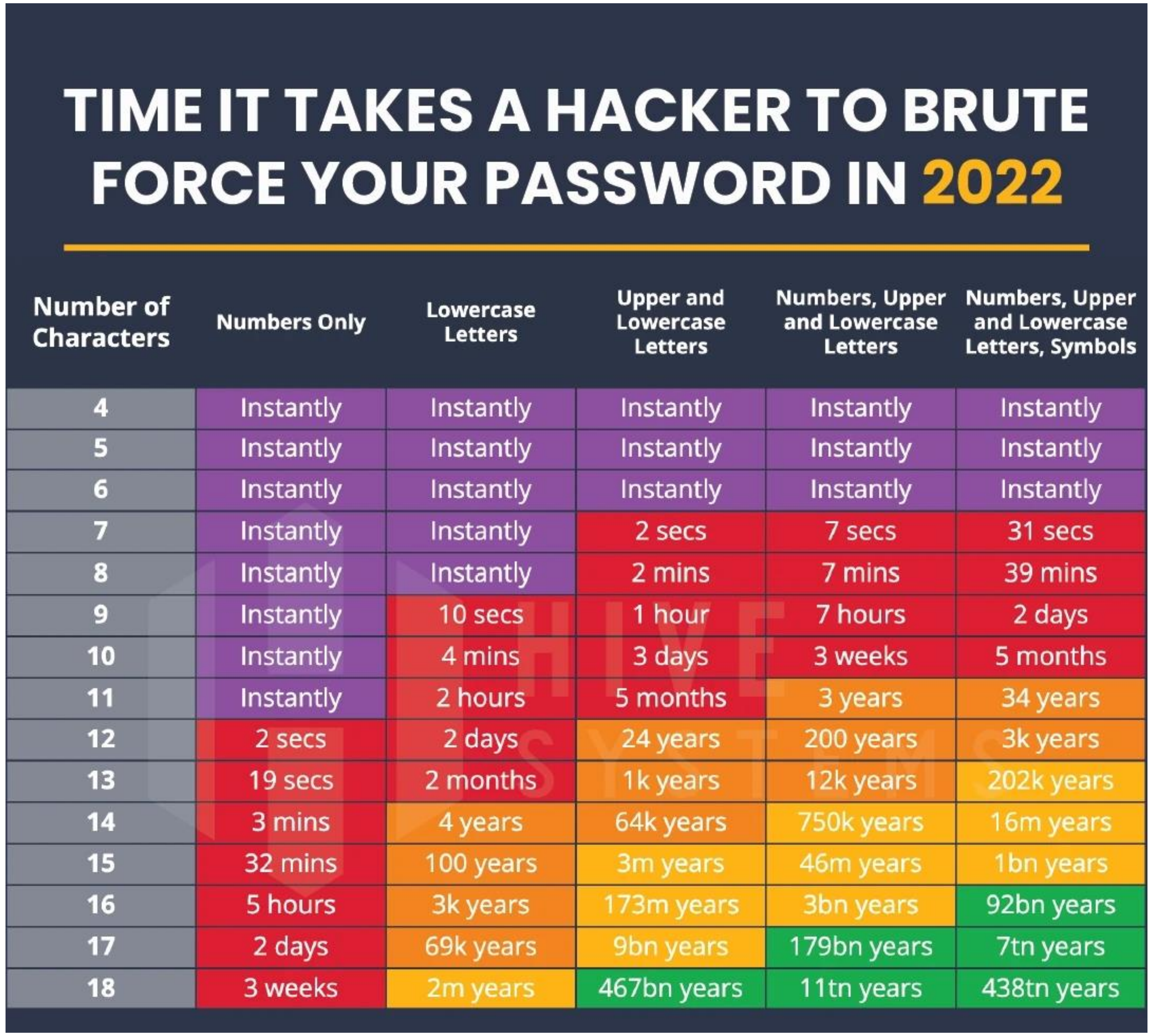
ACTION REQUIRED

Strong passwords

What to avoid?

Top 10 Most Common Passwords
(ones to avoid)

123456
123456789
Qwerty
Password
12345
Qwerty123
1q2w3e
12345678
111111
1234567890



TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2022

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk.

All material is UK Crown Copyright © CITY OF LONDON POLICE: SUITABLE FOR PUBLICATION

Action #1
Use a strong and different password for your email using 3 random words

National Cyber Security Centre
a part of GCHQ

Cyber Aware

Your email password should be strong and different from all your other passwords.

Using 3 random words is a great way to create a password that is easy to remember but hard to crack.

Do not use words that can be guessed (like your pet's name). You can include numbers and symbols if needed.

For example, “HippoPizzaRocket1”

Secure your email password.

Use three random words

HM Government

Cyber Aware

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

ACTION REQUIRED

Action 1:
https://www.ncsc.gov.uk/cyberaware/home

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk.
All material is UK Crown Copyright © CITY OF LONDON POLICE: SUITABLE FOR PUBLICATION

Action #2
Turn on two-step verification (2SV)

National Cyber Security Centre
a part of GCHQ
Cyber Aware

2-Step Verification (2SV) gives you twice the protection.

2SV works by asking for more information to prove your identity.
For example, getting a code sent to your phone or authenticator App

You **won't** be asked for this every time you check your email.

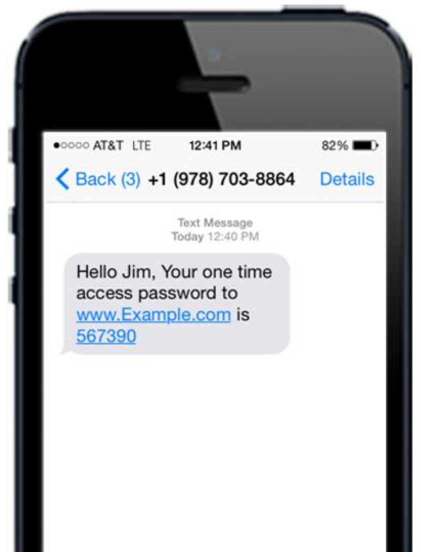
The how:
https://www.ncsc.gov.uk/cyberaware/home#section_4

More detailed information:
https://www.ncsc.gov.uk/guidance/setting-2-step-verification-2sv#section_5

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk.

All material is UK Crown Copyright © CITY OF LONDON POLICE: SUITABLE FOR PUBLICATION

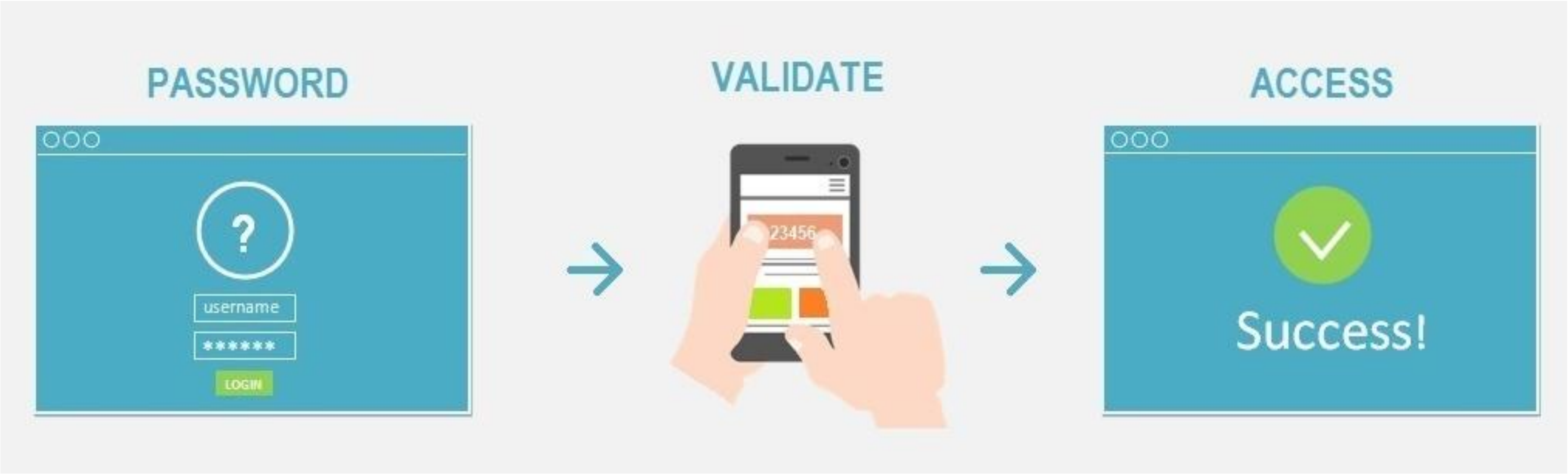
Examples of types of 2SV



Hello Jim, Your one time access password to www.Example.com is 567390

ACTION REQUIRED

- Review your 2SV options
- Secure everything with 2SV:
  - Email accounts
  - Social media
  - Any other online account



This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk.
All material is UK Crown Copyright © CITY OF LONDON POLICE: SUITABLE FOR PUBLICATION

Save your passwords in your browser or using password managers

Using the same password for all your accounts makes you and them vulnerable.

It’s good practice to use different passwords for the accounts you care most

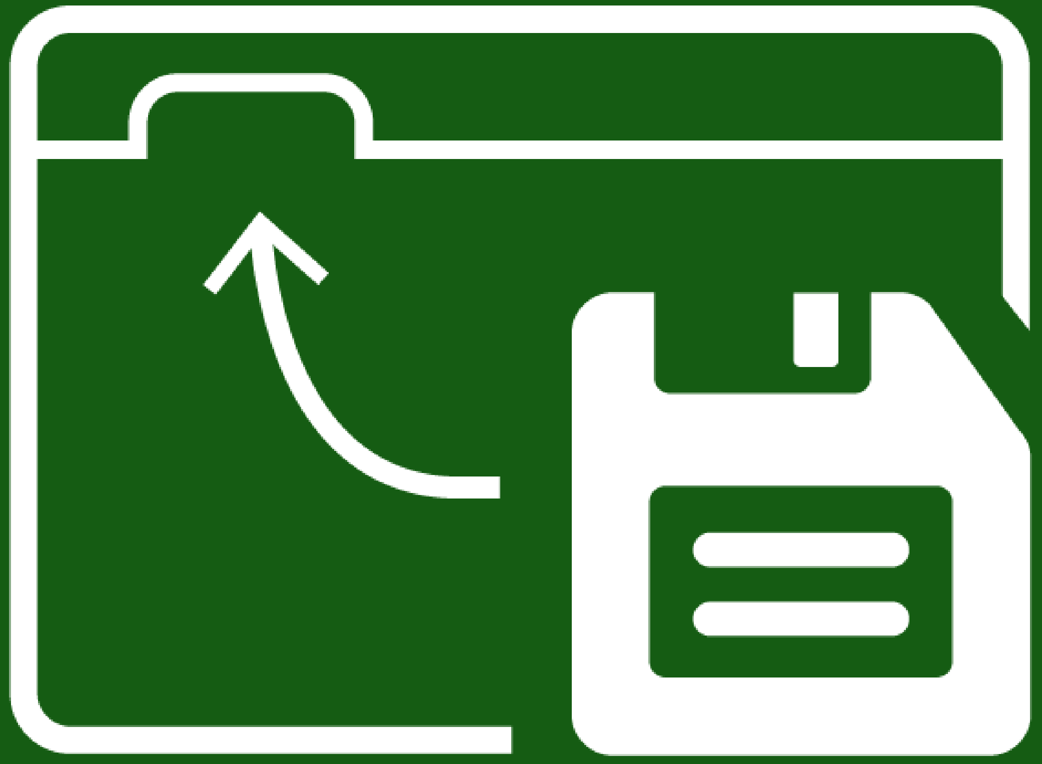
Saving to your browser is quick, convenient and safer than re-using the same password.

Or use a password manager

An App on your phone, tablet or computer that stores your passwords securely.

https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/password-managers

ACTION REQUIRED



Backup up your data

If your phone, tablet or laptop is hacked, your sensitive personal data could be lost, damaged or stolen.

Keep a copy of all your important information by backing it up.

You can back up all your data or only information that is important to you.

ACTION REQUIRED

https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/always-back-up-your-most-important-data

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk.
All material is UK Crown Copyright © CITY OF LONDON POLICE: SUITABLE FOR PUBLICATION

Update your devices

Protect your devices with the latest software updates

Out-of-date software, apps, and operating systems contain weaknesses. This makes them easier to hack. Companies fix the weaknesses by releasing updates. When you update your devices and software, this helps to keep hackers out.

INSTALL

For more information, visit: actionfraud.police.uk/cybercrime

#CyberProtect

https://www.ncsc.gov.uk/guidance/smart-devices-in-the-home

https://www.ncsc.gov.uk/cyberaware#action-5

https://www.ncsc.gov.uk/guidance/smart-security-cameras-using-them-safely-in-your-home

ACTION REQUIRED

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk.
All material is UK Crown Copyright © CITY OF LONDON POLICE: SUITABLE FOR PUBLICATION

Cyber Action Plan Tool

National Cyber Security Centre a part of GCHQ | Cyber Aware

For individuals or sole traders, where you can receive personalised advice on how to improve your online security

https://ncsc.gov.uk/news/consumer-cyber-action-plan…

58% of people are worried about their money being stolen online

53% are worried about having their personal details stolen online

48% are worried about their devices being infected by viruses or malware

Cyber Aware
National Cyber Security Centre
a part of GCHQ

Create a customised Cyber Action Plan today.
National Cyber Security Centre
a part of GCHQ
Cyber Aware

ACTION REQUIRED

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk.
All material is UK Crown Copyright © CITY OF LONDON POLICE: SUITABLE FOR PUBLICATION

Phishing attacks attempt to obtain your personal/private/financial information by email, text, phone and social media.

Ask yourself!

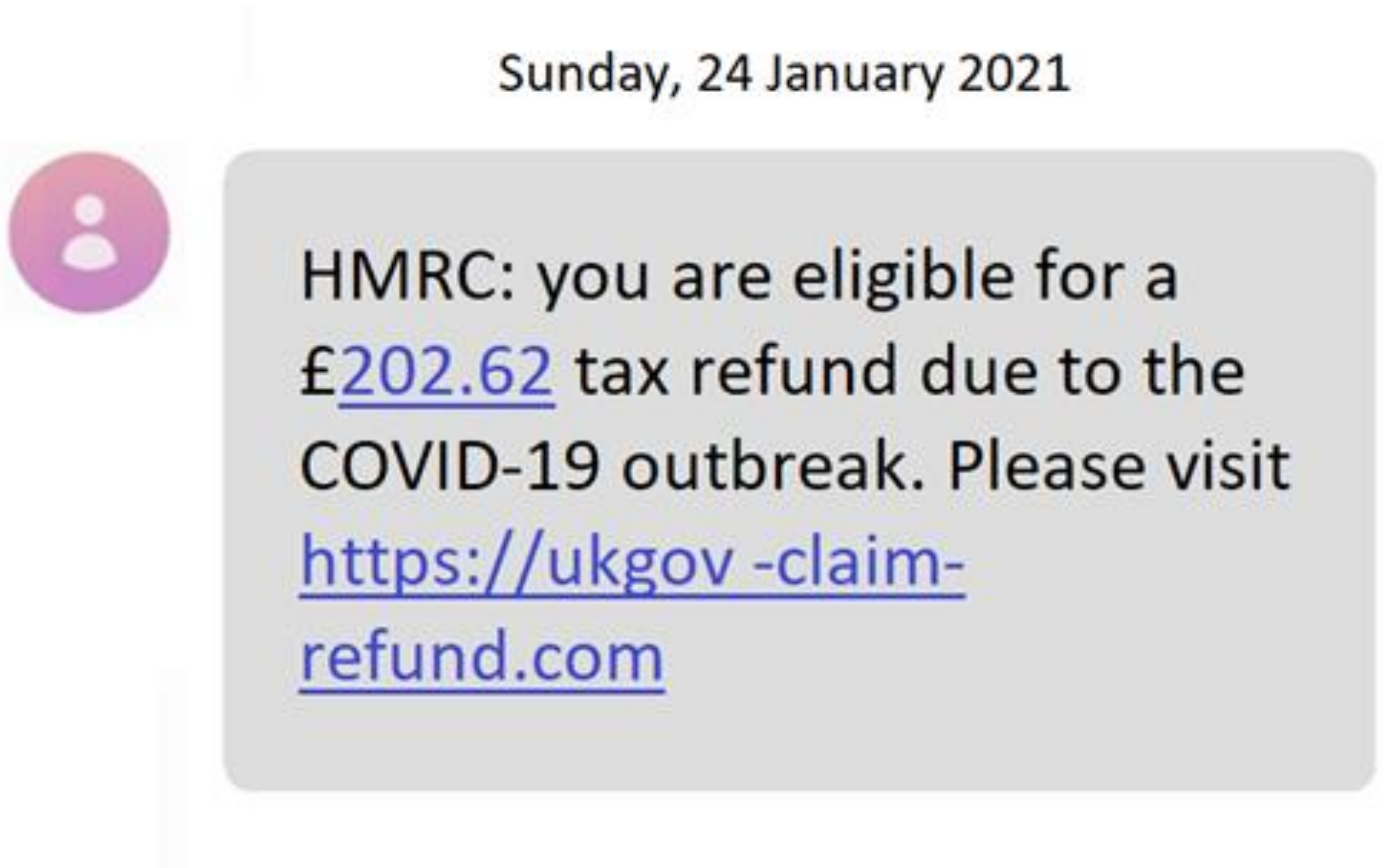
□ **Are you expecting this communication? –** take a moment to think if this company/person would usually contact you.

□ **Look at the senders address/phone number –** sometimes there may be slight spelling changes in email addresses. Always check the website for the correct email and phone number

□ **Avoid clicking links –** even if you are 99% sure, avoid clicking on any links and visit websites directly through your browser.

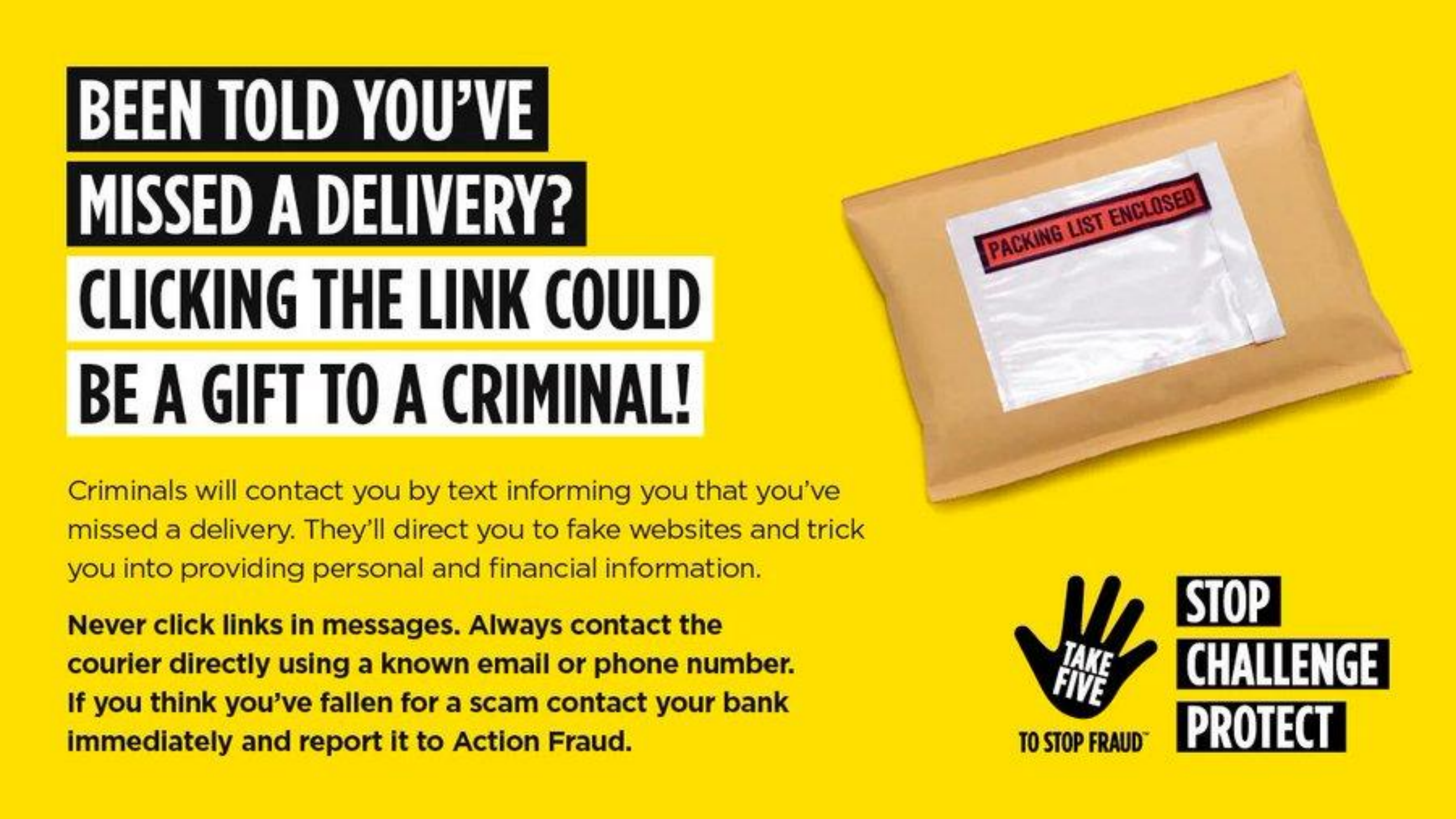
ACTION REQUIRED

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk.
All material is UK Crown Copyright © CITY OF LONDON POLICE: SUITABLE FOR PUBLICATION



Sunday, 24 January 2021

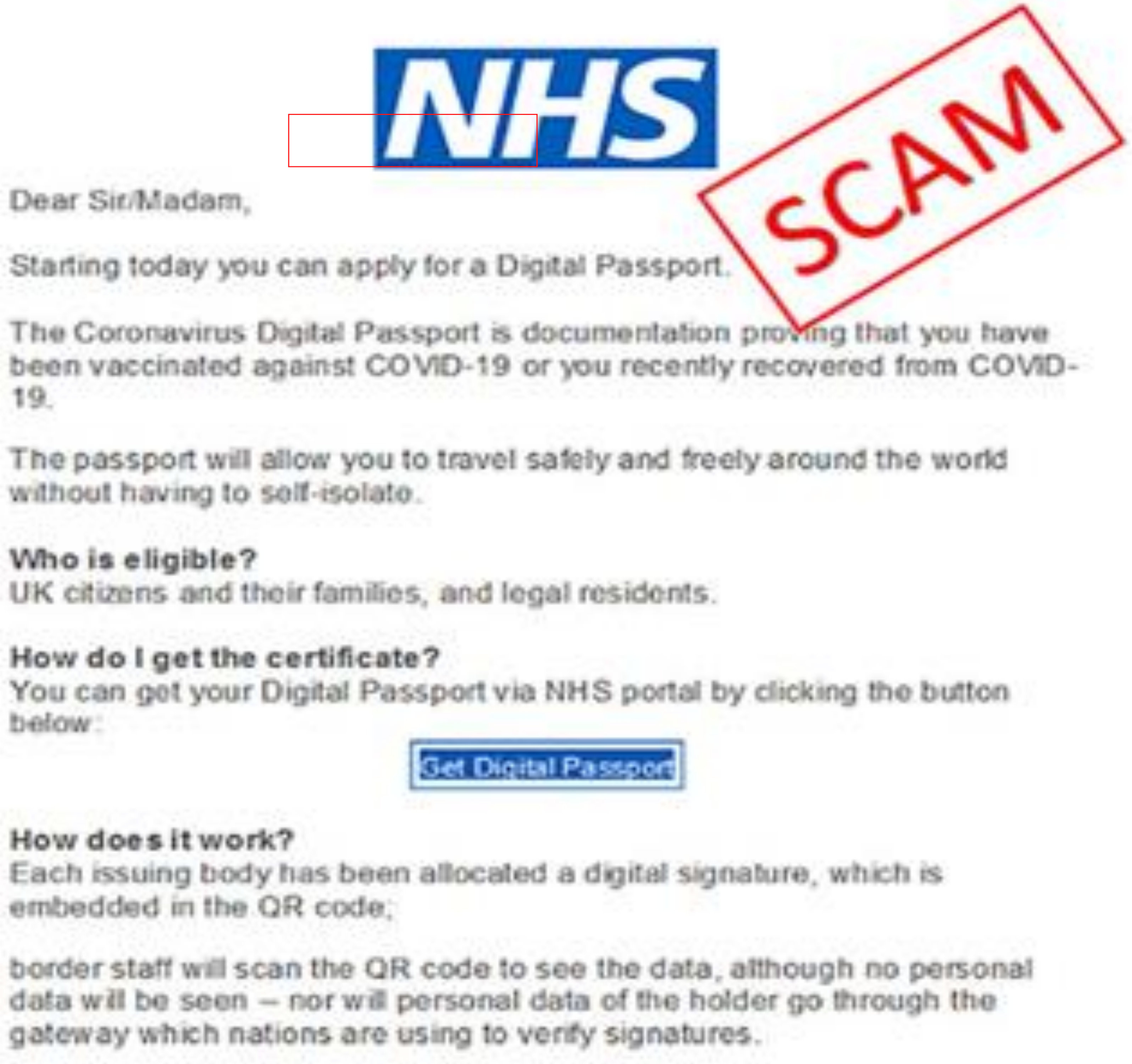
HMRC: you are eligible for a £202.62 tax refund due to the COVID-19 outbreak. Please visit https://ukgov -claim-refund.com



BEEN TOLD YOU'VE MISSED A DELIVERY? CLICKING THE LINK COULD BE A GIFT TO A CRIMINAL!

Criminals will contact you by text informing you that you've missed a delivery. They'll direct you to fake websites and trick you into providing personal and financial information.

Never click links in messages. Always contact the courier directly using a known email or phone number. If you think you've fallen for a scam contact your bank immediately and report it to Action Fraud.



NHS

SCAM

Dear Sir/Madam,

Starting today you can apply for a Digital Passport.

The Coronavirus Digital Passport is documentation proving that you have been vaccinated against COVID-19 or you recently recovered from COVID-19.

The passport will allow you to travel safely and freely around the world without having to self-isolate.

Who is eligible?
UK citizens and their families, and legal residents.

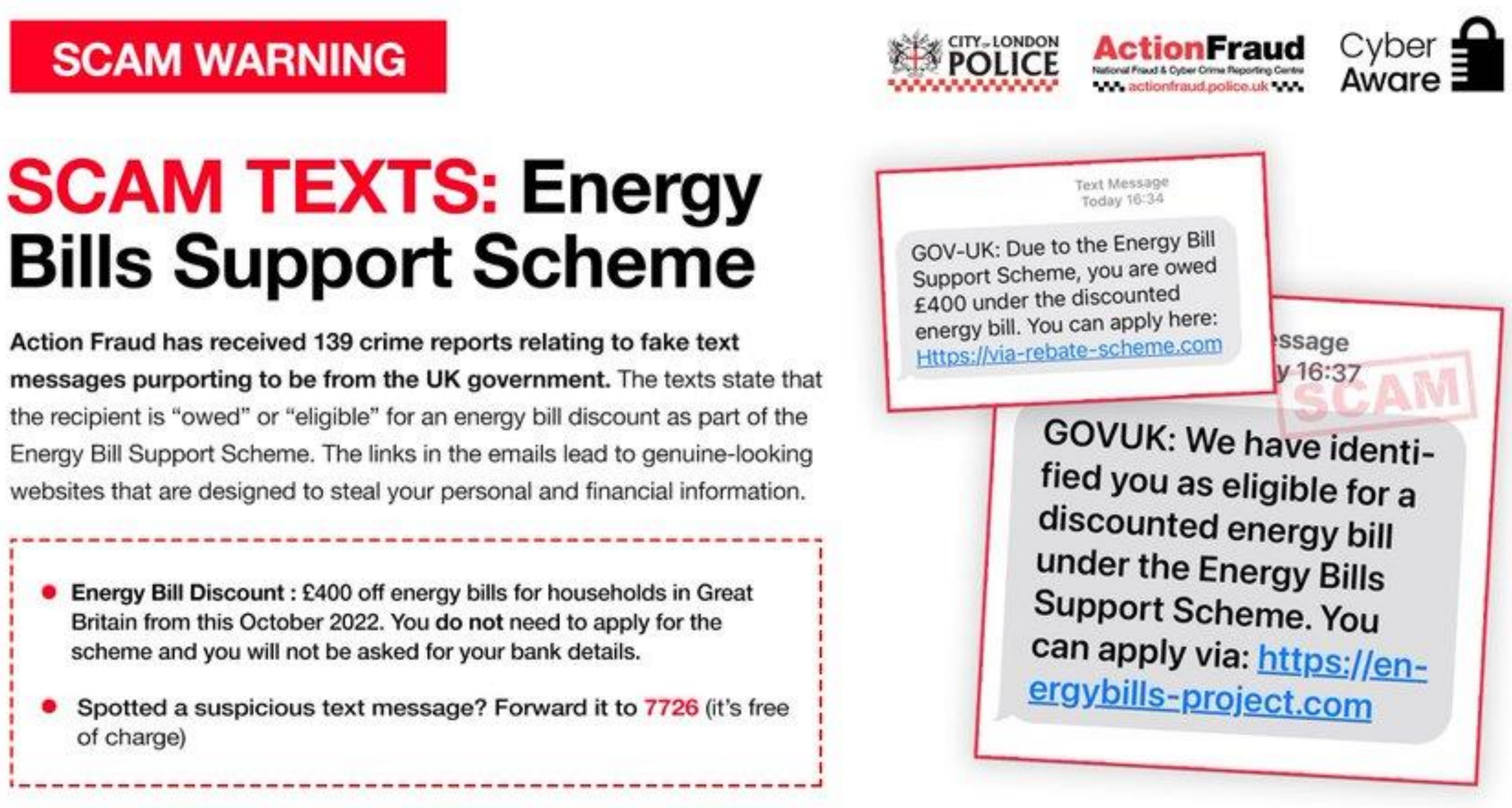
How do I get the certificate?
You can get your Digital Passport via NHS portal by clicking the button below:

Get Digital Passport

How does it work?
Each issuing body has been allocated a digital signature, which is embedded in the QR code;

border staff will scan the QR code to see the data, although no personal data will be seen – nor will personal data of the holder go through the gateway which nations are using to verify signatures.

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk.
All material is UK Crown Copyright © CITY OF LONDON POLICE: SUITABLE FOR PUBLICATION



SCAM WARNING

CITY of LONDON POLICE ActionFraud National Fraud & Cyber Crime Reporting Centre actionfraud.police.uk Cyber Aware

SCAM TEXTS: Energy Bills Support Scheme

Action Fraud has received 139 crime reports relating to fake text messages purporting to be from the UK government. The texts state that the recipient is "owed" or "eligible" for an energy bill discount as part of the Energy Bill Support Scheme. The links in the emails lead to genuine-looking websites that are designed to steal your personal and financial information.

- **Energy Bill Discount :** £400 off energy bills for households in Great Britain from this October 2022. You **do not** need to apply for the scheme and you will not be asked for your bank details.
- Spotted a suspicious text message? Forward it to 7726 (it's free of charge)

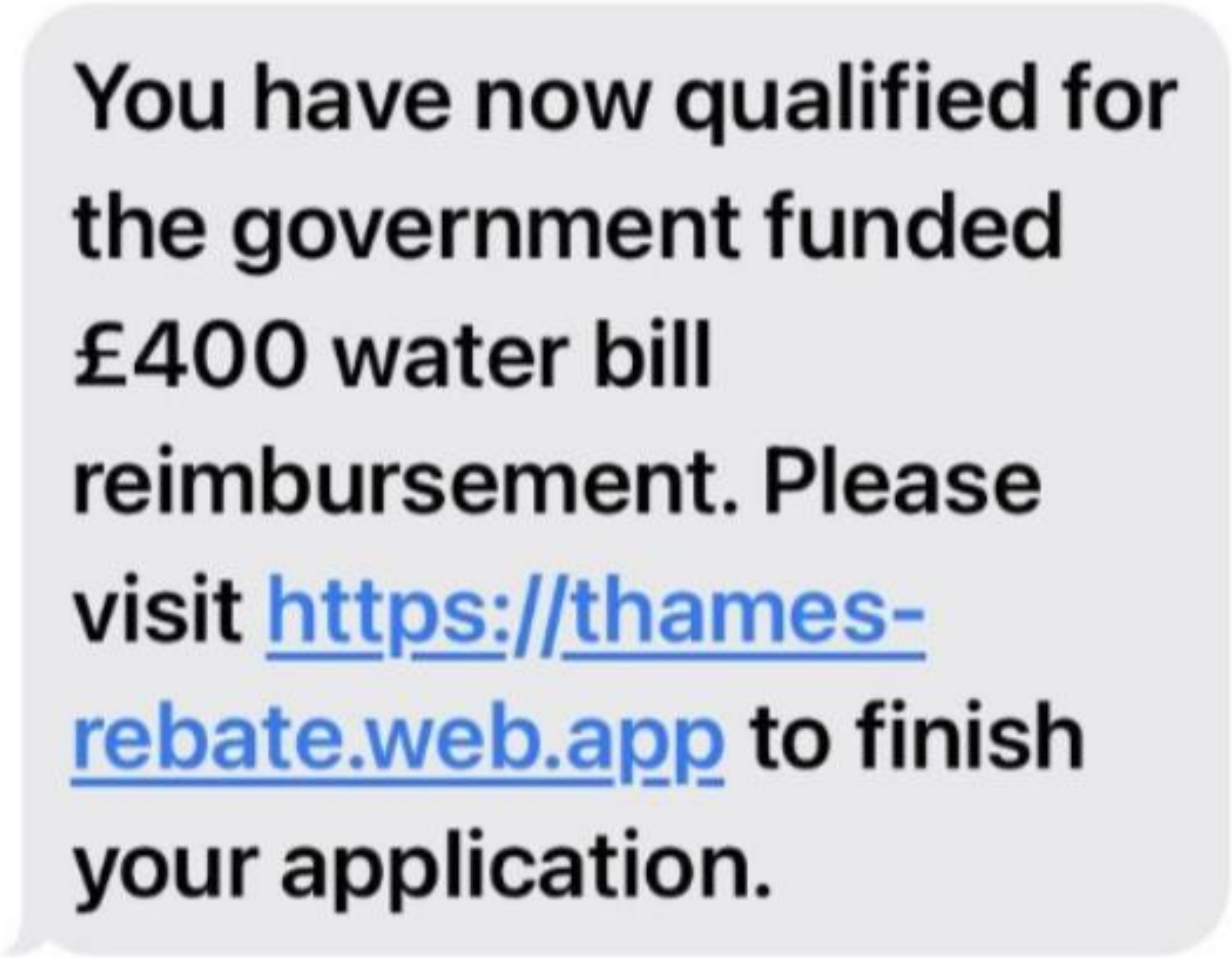
Text Message
Today 16:34

GOV-UK: Due to the Energy Bill Support Scheme, you are owed £400 under the discounted energy bill. You can apply here: Https://via-rebate-scheme.com

essage
y 16:37

SCAM

GOVUK: We have identified you as eligible for a discounted energy bill under the Energy Bills Support Scheme. You can apply via: https://energybills-project.com



You have now qualified for the government funded £400 water bill reimbursement. Please visit https://thames-rebate.web.app to finish your application.

So how can we be tricked

National Cyber Security Centre
a part of GCHQ
Cyber Aware

Sometimes we can be tricked into making impulsive decisions, as criminals use the following tactics:

Urgency – being put under a time limit, or being asked to provide information urgently, does not give us time to think about what is being asked of us.

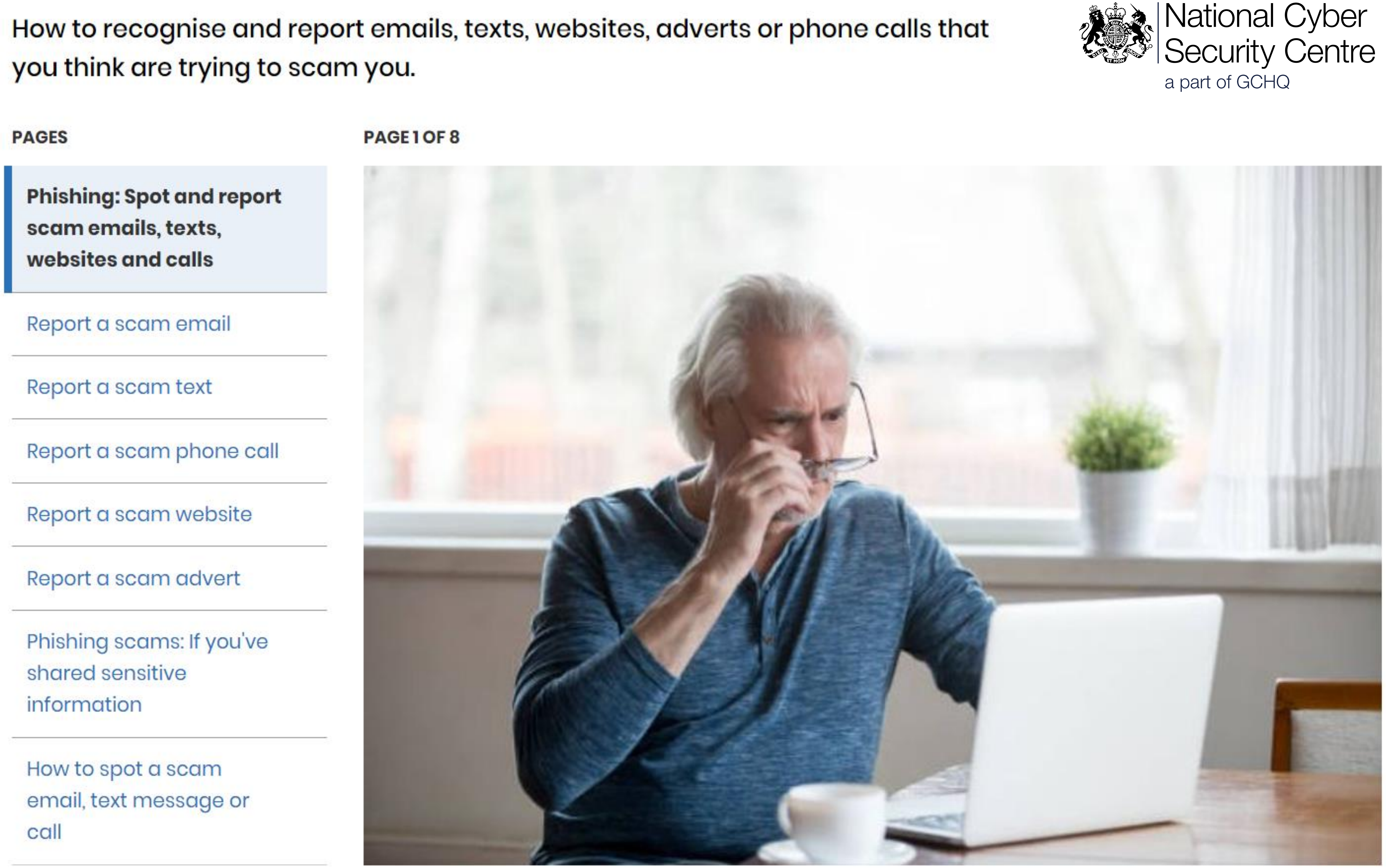
Authority – we may receive a request from someone pertaining to be from an authoritative body, such as the police or bank, which we normally would not think to question.

Trusted organisations – if we receive a request from a ‘company’ or ‘person’ we frequently hear from or shop with, we may not feel to question the legitimacy of the request

Reward - it is easy to fall into a trap of winning a fantastic prize or amount of money. If it looks too good to be true, it probably is!

Emotion – we as people have emotive sides, which can be played upon in scams. Requests from ‘charities’ or ‘friends in need’ should always be double, or triple checked.

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk.
All material is UK Crown Copyright © CITY OF LONDON POLICE: SUITABLE FOR PUBLICATION



How to recognise and report emails, texts, websites, adverts or phone calls that you think are trying to scam you.

PAGES

- **Phishing: Spot and report scam emails, texts, websites and calls**
- Report a scam email
- Report a scam text
- Report a scam phone call
- Report a scam website
- Report a scam advert
- Phishing scams: If you've shared sensitive information
- How to spot a scam email, text message or call

PAGE 1 OF 8

https://www.ncsc.gov.uk/collection/phishing-scams

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk.

All material is UK Crown Copyright © CITY OF LONDON POLICE: SUITABLE FOR PUBLICATION

Phishing Scams

Reporting suspicious messages

National Cyber Security Centre
a part of GCHQ | Cyber Aware

If you are suspicious of an email, report it by forwarding it to:
report@phishing.gov.uk

Checking websites:
https://www.getsafeonline.org/checkawebsite

Report suspicious websites to:
https://www.ncsc.gov.uk/collection/phishing-scams/report-scam-website

If you are suspicious of a text, report it by forwarding it to:
7726

Reporting of nuisance calls to the Information Commissioners Office:
https://ico.org.uk/make-a-complaint/nuisance-calls-and-messages/spam-texts-and-nuisance-calls/

ACTION REQUIRED

Reported an email to the NCSC?

They will
- seek to block the address the email came from
- work with hosting companies to remove links to malicious websites
- raise awareness of commonly reported suspicious emails and methods used (via partners)

Thank you for your continued support.

Report suspicious emails to:
report@phishing.gov.uk
ActionFraud
NPCC
Cyber Aware
209,000
scam websites removed
www.
Updated: January 2023

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk.
All material is UK Crown Copyright © CITY OF LONDON POLICE: SUITABLE FOR PUBLICATION

If you have responded in any way to suspicious emails and Text messages

Banking details? - Contact your bank, let them know.

Account has been hacked? - Refer to the NCSC's guidance on recovering a hacked account.

Occurred on a work laptop or phone? - Contact your IT department.

If you opened a link on your computer? - Open your antivirus (AV) software if you have it, and run a full scan. Allow your antivirus software to clean up any problems it finds.

Given out your password? - Change the passwords on any of your accounts which use the same password.

Lost money? - Tell your bank and report it as a crime to Action Fraud

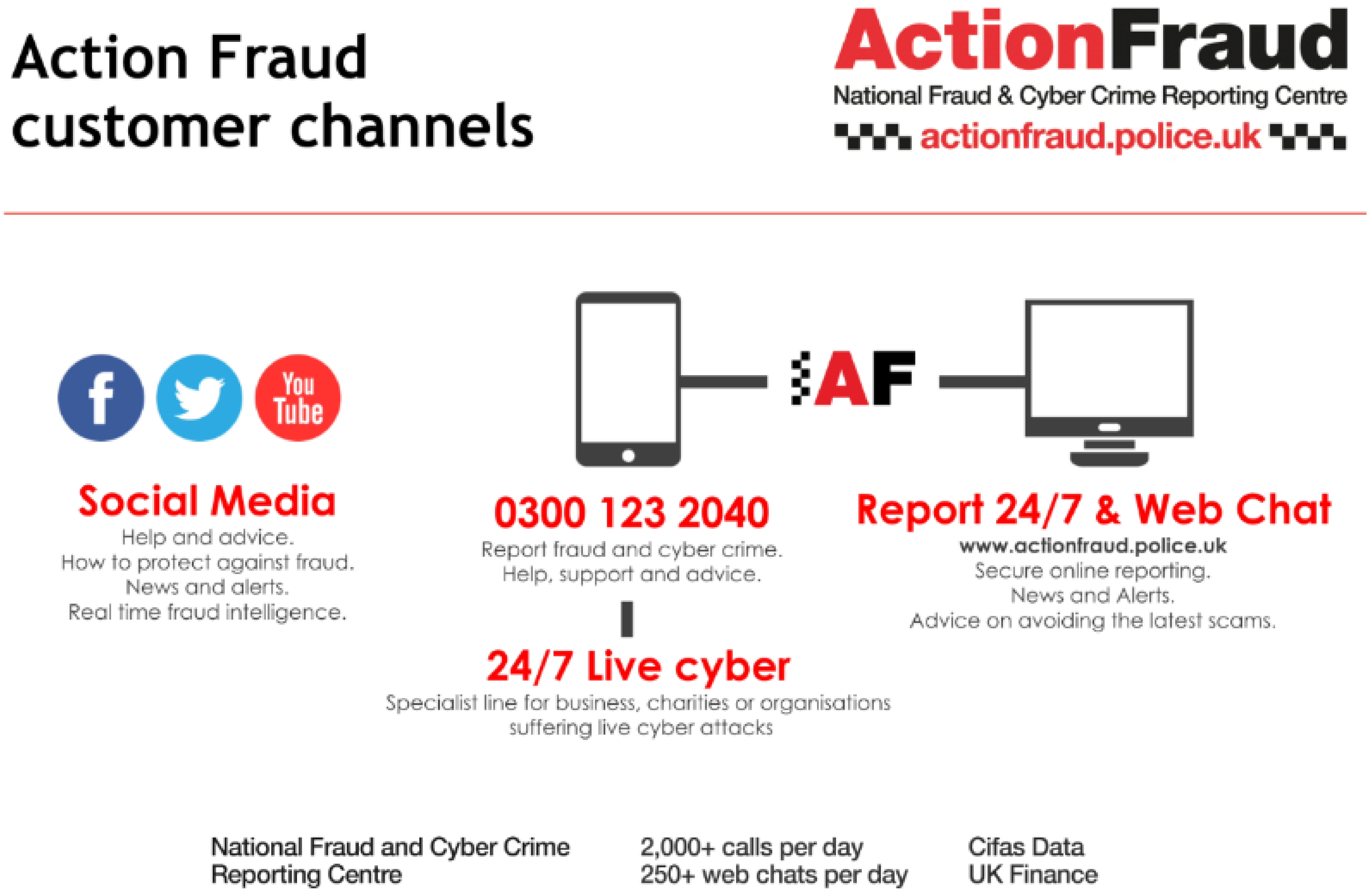
ACTION REQUIRED

Citizens Advice's Scams Action service, visit www.citizensadvice.org.uk

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk.
All material is UK Crown Copyright © CITY OF LONDON POLICE: SUITABLE FOR PUBLICATION

Reporting of Fraud / Cyber Crime

https://www.actionfraud.police.uk/guide-to-reporting



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.

0300 123 2040
Report fraud and cyber crime.
Help, support and advice.

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.

National Fraud and Cyber Crime Reporting Centre

2,000+ calls per day
250+ web chats per day

Cifas Data
UK Finance

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk. All material is UK Crown Copyright © CITY OF LONDON POLICE: SUITABLE FOR PUBLICATION

National Cyber Security Centre
a part of GCHQ
Cyber Aware

Data breaches:

guidance for individuals and families

What is a data breach?
A data breach occurs when information held by an organisation is stolen or accessed without authorisation.

Criminals can then use this information when creating phishing messages (such as emails and texts) so that they appear legitimate.

The message has been designed to make it sound like you're being individually targeted, when in reality the criminals are sending out millions of these scam messages.

Even if your details are not stolen in the data breach, the criminals will exploit high profile breaches (whilst they are still fresh in people's minds) to try and trick people into clicking on scam messages.

Full guidance here: https://www.ncsc.gov.uk/guidance/data-breaches

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk.
All material is UK Crown Copyright © CITY OF LONDON POLICE: SUITABLE FOR PUBLICATION

Smart devices

What is the risk from using Smart Devices?

Just like a smartphone, laptop or PC, smart devices can be hacked to leave your data and privacy at risk. Very rarely, devices have been controlled by somebody else managing the device, often to frighten the victim.

1. Set them up properly
2. Check the default settings
3. Managing your account
4. Keep the device updated

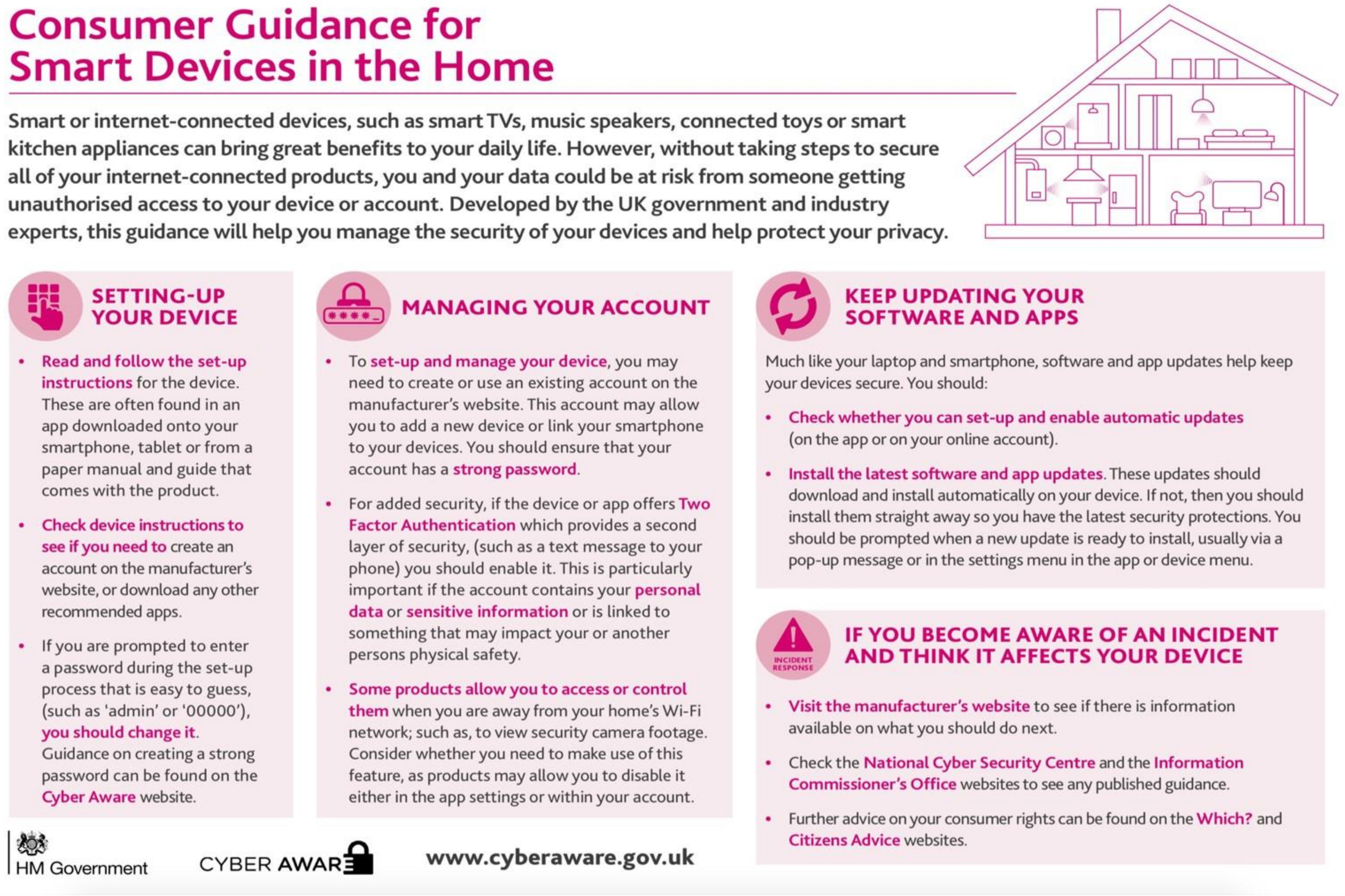
Other considerations

If something goes wrong
Getting rid of your device

More guidance here:
https://www.ncsc.gov.uk/guidance/smart-devices-in-the-home

https://www.ncsc.gov.uk/guidance/smart-security-cameras-using-them-safely-in-your-home

https://www.ncsc.gov.uk/guidance/buying-selling-second-hand-devices



Consumer Guidance for Smart Devices in the Home

Smart or internet-connected devices, such as smart TVs, music speakers, connected toys or smart kitchen appliances can bring great benefits to your daily life. However, without taking steps to secure all of your internet-connected products, you and your data could be at risk from someone getting unauthorised access to your device or account. Developed by the UK government and industry experts, this guidance will help you manage the security of your devices and help protect your privacy.

SETTING-UP YOUR DEVICE

- **Read and follow the set-up instructions** for the device. These are often found in an app downloaded onto your smartphone, tablet or from a paper manual and guide that comes with the product.
- **Check device instructions to see if you need to** create an account on the manufacturer's website, or download any other recommended apps.
- If you are prompted to enter a password during the set-up process that is easy to guess, (such as 'admin' or '00000'), **you should change it**. Guidance on creating a strong password can be found on the **Cyber Aware** website.

MANAGING YOUR ACCOUNT

- To **set-up and manage your device**, you may need to create or use an existing account on the manufacturer's website. This account may allow you to add a new device or link your smartphone to your devices. You should ensure that your account has a **strong password**.
- For added security, if the device or app offers **Two Factor Authentication** which provides a second layer of security, (such as a text message to your phone) you should enable it. This is particularly important if the account contains your **personal data** or **sensitive information** or is linked to something that may impact your or another persons physical safety.
- **Some products allow you to access or control them** when you are away from your home's Wi-Fi network; such as, to view security camera footage. Consider whether you need to make use of this feature, as products may allow you to disable it either in the app settings or within your account.

KEEP UPDATING YOUR SOFTWARE AND APPS

Much like your laptop and smartphone, software and app updates help keep your devices secure. You should:

- **Check whether you can set-up and enable automatic updates** (on the app or on your online account).
- **Install the latest software and app updates**. These updates should download and install automatically on your device. If not, then you should install them straight away so you have the latest security protections. You should be prompted when a new update is ready to install, usually via a pop-up message or in the settings menu in the app or device menu.

IF YOU BECOME AWARE OF AN INCIDENT AND THINK IT AFFECTS YOUR DEVICE

INCIDENT RESPONSE

- **Visit the manufacturer's website** to see if there is information available on what you should do next.
- Check the **National Cyber Security Centre** and the **Information Commissioner's Office** websites to see any published guidance.
- Further advice on your consumer rights can be found on the **Which?** and **Citizens Advice** websites.

HM Government CYBER AWARE www.cyberaware.gov.uk

ACTION REQUIRED

All material is UK Crown Copyright © CITY OF LONDON POLICE: SUITABLE FOR PUBLICATION

Social media – how to use if safely

National Cyber Security Centre
a part of GCHQ

Cyber Aware

1. Advice from the social media platform
2. Use 2SV (2 Step verification) to protect the accounts
3. Understanding your digital footprint
4. Spotting and reporting fake accounts
5. Social media and children:

https://www.internetmatters.org/parental-controls/social-media/

#TurnOn2SV
14,493 people reported their email or social media accounts hacked*
* Reported in financial year 2021-2022

Email and social media account passwords should be **strong and different from all your other passwords.** Enabling 2-step verification (2SV) will keep criminals out of your account, even if your password is stolen.

Working in partnership to protect the UK public and businesses from fraud and cyber crime.

Full guidance here: https://www.ncsc.gov.uk/guidance/social-media-how-to-use-it-safely

ACTION REQUIRED

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk.

All material is UK Crown Copyright © CITY OF LONDON POLICE: SUITABLE FOR PUBLICATION

Shopping online securely

How to shop safely online.

National Cyber
Security Centre
a part of GCHQ

Cyber
Aware

1. Choose carefully where you shop online

2. Use a credit card for online payments

Section 75: credit card payment protection If you use your credit card to buy something, including goods or a holiday (even if you only put the deposit on your credit card), costing over £100 and up to £30,000, you're covered by 'section 75' of the Consumer Credit Act. This means the credit card company has equal responsibility (or 'liability') with the seller if there's a problem with the things you've bought or the company you've bought them from fails.

1. Only provide enough details to complete the purchase

2. Keep your account secure (See Cyber Aware)

3. Watch out for suspicious email, text messages and websites(See NCSC)

4. If things go wrong

If you don't receive the item (or it doesn't match the description given),
Citizens Advice has some useful information about getting your money back if you paid by credit card, debit card or PayPal

https://www.ncsc.gov.uk/guidance/shopping-online-securely

https://www.citizensadvice.org.uk/consumer/somethings-gone-wrong-with-a-purchase/getting-your-money-back-if-you-paid-by-card-or-paypal/

ACTION REQUIRED

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk.
All material is UK Crown Copyright © CITY OF LONDON POLICE: SUITABLE FOR PUBLICATION

Summary of guidance for individuals

Aim: To have an understanding of and have a behavioural change toward:

Take your email security to another level.

Advice on how to stay secure online from the UK's National Cyber Security Centre

National Cyber
Security Centre
Cyber
Aware

Cyber Aware has all of the above information in greater detail and with help sections: https://www.ncsc.gov.uk/cyberaware/home

Report Suspicious Emails to: report@phishing.gov.uk **Report Suspicious texts**, by forwarding them to **7726**

Report Suspicious websites: https://www.ncsc.gov.uk/collection/phishing-scams/report-scam-website

Reporting of Fraud / Cyber Crime – Action Fraud: https://www.actionfraud.police.uk/guide-to-reporting

Additional Cyber Security guidance: https://www.ncsc.gov.uk/section/information-for/individuals-families

From our Regional Pages: https://serocu.police.uk/individuals/

Be also aware of door step, romance, computer service, get rich quick fraud & other rogue trader offences.

“Too good to be true? Then Yes it’s a Scam!!”

Advice and support from Citizens Advice’s Scams Action service: https://www.citizensadvice.org.uk/

Reporting of nuisance calls to the Information Commissioners Office:
https://ico.org.uk/make-a-complaint/nuisance-calls-and-messages/spam-texts-and-nuisance-calls/

National Cyber Security Centre
a part of GCHQ
Cyber Aware

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk. All material is UK Crown Copyright © CITY OF LONDON POLICE: SUITABLE FOR PUBLICATION

Thank you for this opportunity to have presented the above content to you

Get the latest information and reports from the **National Cyber Security Centre, Action Fraud and TVP**

- Cyber Alerts & Advisories: www.ncsc.gov.uk/index/alerts-and-advisories
- Surrey Police Neighbourhood Alerts / In the Know: https://www.intheknow.community
- Action Fraud Alerts: https://www.actionfraud.police.uk/sign-up-for-action-fraud-alert

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk.
All material is UK Crown Copyright © CITY OF LONDON POLICE: SUITABLE FOR PUBLICATION