Cyber Crime and Fraud

The Threats to UK Businesses

Report Fraud

CITY OF LONDON POLICE

ANNETTE WEST: PROTECT SUPERVISOR
(CYBER CRIME & FRAUD)

OFFICIAL

Wales and South West Credit Management Conference 19.03.2026

The Scale of the Threat 2024-25

Fraud is the single **biggest** crime type in the UK

43% of businesses reported a cyber breach or attack in the last 12 months

Fraud makes up **39%** of all crime

This rises to **50%** with cyber crime included

- 336,207 fraud reports
- £2.6bn fraud losses
- 67% of fraud is cyber enabled
- 90% of fraud has an online element with growing prevalence of AI
- 48,314 cyber Crimes reported
- £7.5mil cyber losses
- 1 in 2 businesses suffer cyber breaches

Top Threats To Businesses

- Ransomware
- Phishing
- Payment Diversion Fraud

1

Ransomware

Report Fraud

CITY OF LONDON POLICE

Ransomware

Ransomware is a type of malware which prevents you from accessing your device and the data stored on it, usually by encrypting your files. A criminal group will then demand a ransom in exchange for decryption.

Reporting Trends and Threats to Businesses

Ransomware attacks were one of the most prolific crimes targeting organisations in 2025, Ransomware-as-a-Service (RaaS) is becoming a growing issue as technology advances.

Companies account for **96%** of the ransomware reports made to Report Fraud.

Ransomware among businesses significantly increased between 2024 and 2025. It is estimated that **19,000** businesses experienced a ransomware crime in the last 12 months in 2025.

AI-driven ransomware emerged as a major cybersecurity threat in 2025, with several ransomware groups leveraging machine learning and automation to enhance their attacks.

48 new ransomware groups were identified in 2024-25.

2 new ransomware variants were identified in **January 2026** ‘Beast’ and ‘Bajahai’ The Beast operates under a Ransomware-as-a-Service model, first believed to have launched in winter 2024,rapidly evolving throughout 2025.

RANSOMWARE is vastly under reported to Report Fraud

The Mini Guide to Ransomware

One of the biggest current threats in cybercrime is ransomware.

Case Study: Ransomware

In **January 2026** intelligence was received on a company who had been a victim of an **Interlock ransomware attack**, being named on that ransomware group's data leak site. The threat actor claimed to have access to **941GB** of data.

Initial contact was made by the National Crime Agency, who then tasked the incident to the regional organised crime unit covering the location in which the organisation was based. Protect officers conducted a visit to the organisation within **24 hours** of receiving the intelligence. Initially the organisation did not believe that they were the police and thought they were part of the threat actor group (due to lack of detail from the NCA). Upon arrival the officers were trapped in a car park and were not allowed into the building until the organisation phoned the local response police to verify.

The protect officers were then able to reassure the organisation and gain access to speak with the IT manager, who confirmed they were aware of the incident. The organisation believed the attack was activated in December and had performed necessary steps to recover and restore servers, changed passwords, implemented 2SV, removed affected PCs, ran antivirus system scans, contacted customers… and reported to Report Fraud.

After the initial hesitation the organisation were then willing to work with the police protect officers and arranged a follow up meeting. The organisation have since requested that the protect officers engage further with their staff members, The officers were also able to share information with the organisation on how to access the data leak site and view their files, they also provided detailed mitigation advice.

Ransomware Prevention and Recovery

www.ncsc.gov.uk

Don't be blackmailed - keep a backup!

If you have a recent backup of your most important files, then you can't be blackmailed.

Make regular backups of your most important files (such as photos and documents), and check that you know how to restore the files from the backup. If you're unsure how to do this, you can search online.

Make sure the device containing your backup (such as an external hard drive or a USB stick) **is not permanently connected** to your computer.

Turn on auto-backup so that data on your smartphone is automatically copied to the cloud. This means you'll be able to recover your data quickly by signing back into your account from another device.

Protecting your data and devices

The following steps will reduce the likelihood of your devices being infected with ransomware.

Keep your operating system and apps up to date. Apply software updates promptly to help keep your device secure. This includes protection from ransomware and other types of virus. Set updates to happen automatically, so you don't forget.

Make sure your antivirus product is turned on and up to date. Windows and macOS have built in malware protection tools which are suitable for this purpose.

Avoid downloading dodgy apps. Only use official app stores (like Google Play or the Apple App Store), which provide protection from viruses.

What to do if you are infected

If your computer has been infected by ransomware (or any type of malware), you should:

Open your antivirus (AV) software, **and run a full scan**. Follow any instructions given. If your AV can't clean your device, you'll need to perform a 'clean re-install', which will remove all your personal files, apps and settings. If you're unsure how to do this, you can search online using another device, or ask family and friends.

Restore your backed-up data that you have kept on a separate device (such as USB stick, external hard drive) or cloud storage. Do not copy any data from the infected computer.

If you receive a phone call offering help to clean up your computer, **hang up immediately** (this is a common scam).

Anyone who thinks they may be have been subject to a ransomware attack should **contact Report Fraud** (www.reportfraud.police.uk) 0300 123 2040. In Scotland, contact the police by dialing 101

Should I pay the ransom?

Law enforcement do not encourage, endorse, nor condone the payment of ransom demands. If you do pay the ransom:

- there is no guarantee that you will get access to your data or computer
- your computer will still be infected
- you will be paying criminal groups
- you're more likely to be targeted in the future

If you have paid any extortion demands you should report this to your local police force.

2

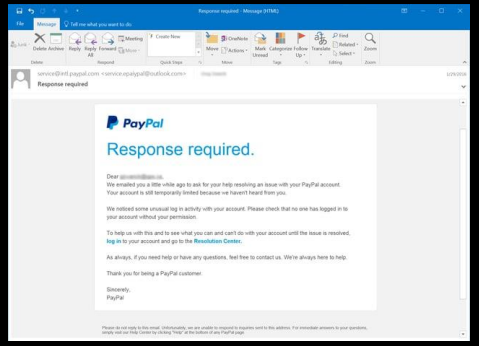
Phishing

Report Fraud

CITY OF LONDON POLICE

Phishing

Phishing is a form of social engineering in which attackers create deceptive messages that appear to be from legitimate sources to harvest sensitive information or install malware, and as such is the most used attack vector in online fraud.



Reporting Trends and Threats to Businesses

Phishing is the primary, most common, and most effective vector for delivering **ransomware**, with reports in 2025 showing it accounts for **35%** of all ransomware incidents, and over **90%** of successful cyber attacks start with a phishing email.

Phishing is the most used attack vector in online fraud.

Predictions warn that AI powered social-engineering will ‘surge and fuel **ransomware** campaigns’, with voice-phishing (vishing) leveraging generative-AI voices that mimic local accents and dialects to convince employees into granting access.

Report Fraud received **3,744** reports of phishing in 2024/25, a total of **£42 million** was reported as lost to phishing, with an average of **£35,000** lost per victim.

7.87 million phishing attacks in 2025 (cyber security breaches survey).

Anatomy of Phishing

Broad Attack Vector

Phishing

Messages are sent or calls made en masse

- Messages are not personalised
- May be followed up with Spear Phishing

Often acquired from data:

- Available in the public domain
- Leaked or stolen from breaches elsewhere

Targeted Attack Vector

Spear Phishing

Personalised to the target(s)
Research Required

- Personalised to a specific target
- More believable

Additional Vectors:

- Business E-Mail Compromise
- Potentially followed up with further attacks

Whaling

Targeted at high-level decision makers.

Defending Your Organisation From Phishing

www.ncsc.gov.uk/guidance/phishing

Phishing attacks:
Defending your organisation

National Cyber Security Centre
a part of GCHQ

A multi-layered approach - such as the one summarised below - can improve your resilience against phishing whilst minimising disruption to user productivity. This approach provides multiple opportunities to detect a phishing attack and stop it before it causes major harm. The mitigations included are also useful against other types of cyber attack.

LAYER 1
Make it difficult for attackers to reach users.

- Implement anti-spoofing controls to stop your email addresses being a resource for attackers.
- Consider what information is available to attackers on your website and social media and help your users do the same
- Filter or block incoming phishing emails.

LAYER 2
Help users identify and report suspected phishing emails.

- Relevant training can help users spot phishing emails, but no amount of training can help them spot every email.
- Help users to recognise fraudulent requests by reviewing processes that could be mimicked and exploited.
- Create an environment that lets users seek help through a clear reporting method, useful feedback and a no-blame culture.

LAYER 3
Protect your organisation from the effects of undetected phishing emails.

- Protect your accounts: make authentication more resistant to phishing (such as setting up MFA) and ensure authorisation only gives privileges to people who need them.
- Protect users from malicious websites by using a proxy services and an up-to-date browser.
- Protect your devices from malware.

LAYER 4
Respond to incidents quickly.

- Define and rehearse an incident response plan for different types of incidents, including legal and regulatory responsibilities.
- Detect incidents quickly by encouraging users to report any suspicious activity.

Why you should report suspicious emails

Forward suspicious emails to:

report@phishing.gov.uk

Forward suspicious texts to:

7726

The National Cyber Security Centre (NCSC) has the power to investigate and remove fraudulent email addresses and websites.

By reporting phishing attempts you can:

- reduce the amount of scam emails you receive
- make yourself a harder target for scammers
- protect others from cyber crime online

As of January 2026, the number of reports received stands at:

51m
Reported Scams

Resulting in
241k
Scams being removed

Across
430,000
URLS

3

Payment Diversion Fraud

Report Fraud

CITY OF LONDON POLICE

Payment Diversion Fraud

Payment Diversion Fraud (PDF) is the act of an offender manipulating a victim by gaining their trust to change the course of a payment to an account handled by the offender. Also known as Business Email Compromise (BEC)

Key Stats 2024/25

3,544 reports of PDF to Report Fraud in 2024-25

£134 million in losses
Average loss **£38,000** per case

Thirteen reports included losses of over a million GBP, with the highest loss reported being **£15 million** in one attack.

It is highly likely that the reports received by Report Fraud is a snapshot of the true scale of PDF committed within the UK against individuals and businesses.

These frauds come in several forms, including:

CEO fraud: Criminals impersonate senior executives, sometimes using deepfake audio or video, to pressure staff into making urgent payments.

Invoice fraud: Fraudsters hack supplier email accounts or create lookalike domains to send fake invoices with updated bank details.

Salary diversion fraud: Scammers pose as employees and ask HR or payroll teams to change bank details, redirecting salary payments to their own accounts

Payment diversion fraud is one of the most damaging frauds facing UK businesses today. Criminals deceive staff into sending money to the wrong bank account.


POLICE

PDF The Current Picture – January 2026

339
PDF Reports

109
(32%) Were From Businesses

£6,504,967
Total Losses

Top 3 Reports in January 2026

PDF Categorisation	Losses	No. Of Reports
Invoice Fraud	**£3,004,350**	67
Salary Diversion Fraud	**£134,870**	13
CEO Impersonation	**£80,840**	5

Sector Breakdown

the most frequently reported sectors by the top 4 volumes of reports within the 109 organisational reports. There were 72 reports which provided no sector information.

Sector	Losses	Count	Rank By Volume	Previous Month Rank
Construction	£50,060	6	1st (-)	1st (5)
Information & Communication	£185,200	4	2nd (↑)	5th (1)
Wholesale and Retail Trade, Repair of Motor Vehicles and Motorcycles	£28,720	4	2nd (↑)	5th (1)
Accommodation and Food Services Activities	£1,039	3	3rd (↑)	5th (1)
Arts, Entertainment & Recreation	£130,110	3	3rd (↑)	3rd (3)
Financial and Insurance Activities	£82,100	3	4th (↑)	NS**
Electricity, Gas, Steam, and Air Conditioning Supply	£5,600	2	4th (↑)	NS**
Manufacturing	£363,270	2	4th (↑)	5th (1)
Professional, Scientific & Technical Analysis	£4,817	2	4th (↑)	NS**
Transportation and Storage	£27,600	2	4th (↑)	NS**
Grand Total	£877,516	31		

Payment Diversion Fraud

Future/Emerging Threats

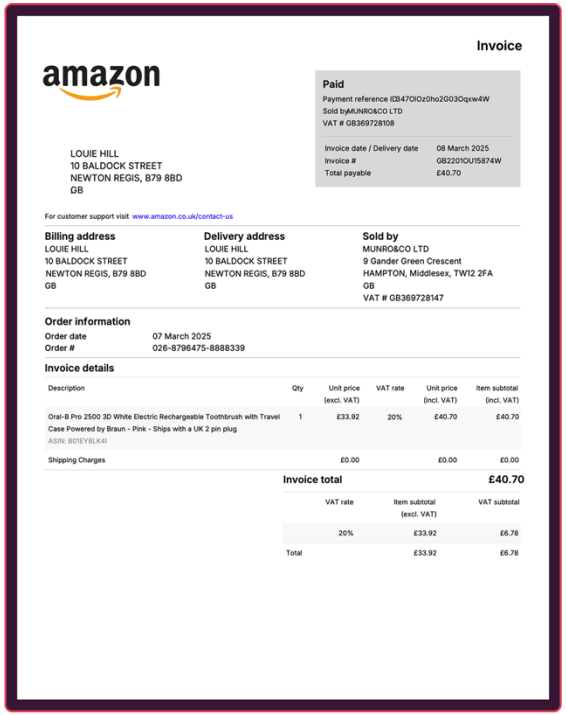
The use of AI

It is almost certain AI will play an important part in bridging the gap between simple and sophisticated PDF offences. An example is the use of generative AI to create deep fakes in real time, changing both the appearance and voice of the offender to impersonate a third party and instil trust in the victim. The expectation is this will increasingly be used by offenders, specifically within CEO fraud typologies, to increase the success rate. Coupled with social engineering techniques and applied pressure, AI may lead to victims proceeding with instructions without due consideration.

Cybercrime-As-a-Service (CaaS)

CaaS has risen to prominence in recent reporting periods and is likely to play a part in the future of PDF; the development and sale of phishing kits will provide criminals without the necessary skillset the ability to target organisations and individuals in payment diversion attacks who otherwise would not have engaged in such criminality.

Protecting your business from payment diversion fraud



Invoice

amazon

Paid
Payment reference ID347OlOz0ho2GO3Oqxw4W
Sold by MUNRO&CO LTD
VAT # GB369728108

Invoice date / Delivery date 08 March 2025
Invoice # GB2201OU15874W
Total payable £40.70

LOUIE HILL
10 BALDOCK STREET
NEWTON REGIS, B79 8BD
GB

For customer support visit www.amazon.co.uk/contact-us

Billing address
LOUIE HILL
10 BALDOCK STREET
NEWTON REGIS, B79 8BD
GB

Delivery address
LOUIE HILL
10 BALDOCK STREET
NEWTON REGIS, B79 8BD
GB

Sold by
MUNRO&CO LTD
9 Gander Green Crescent
HAMPTON, Middlesex, TW12 2FA
GB
VAT # GB369728147

Order information
Order date 07 March 2025
Order # 026-8796475-8888339

Invoice details

Description	Qty	Unit price (excl. VAT)	VAT rate	Unit price (incl. VAT)	Item subtotal (incl. VAT)
Oral-B Pro 2500 3D White Electric Rechargeable Toothbrush with Travel Case Powered by Braun - Pink - Ships with a UK 2 pin plug ASIN: B01EY8LK4I	1	£33.92	20%	£40.70	£40.70
Shipping Charges		£0.00		£0.00	£0.00

Invoice total £40.70

VAT rate	Item subtotal (excl. VAT)	VAT subtotal
20%	£33.92	£6.78
Total	£33.92	£6.78

1. **Be cautious with bank detail changes**
2. **Verify with a trusted contact**
3. **Set up clear procedures**
4. **Secure Supplier Communications**
5. **Communicate Clearly**

STAY VIGILANT ⚠

4

Reporting Cyber Crime and Fraud

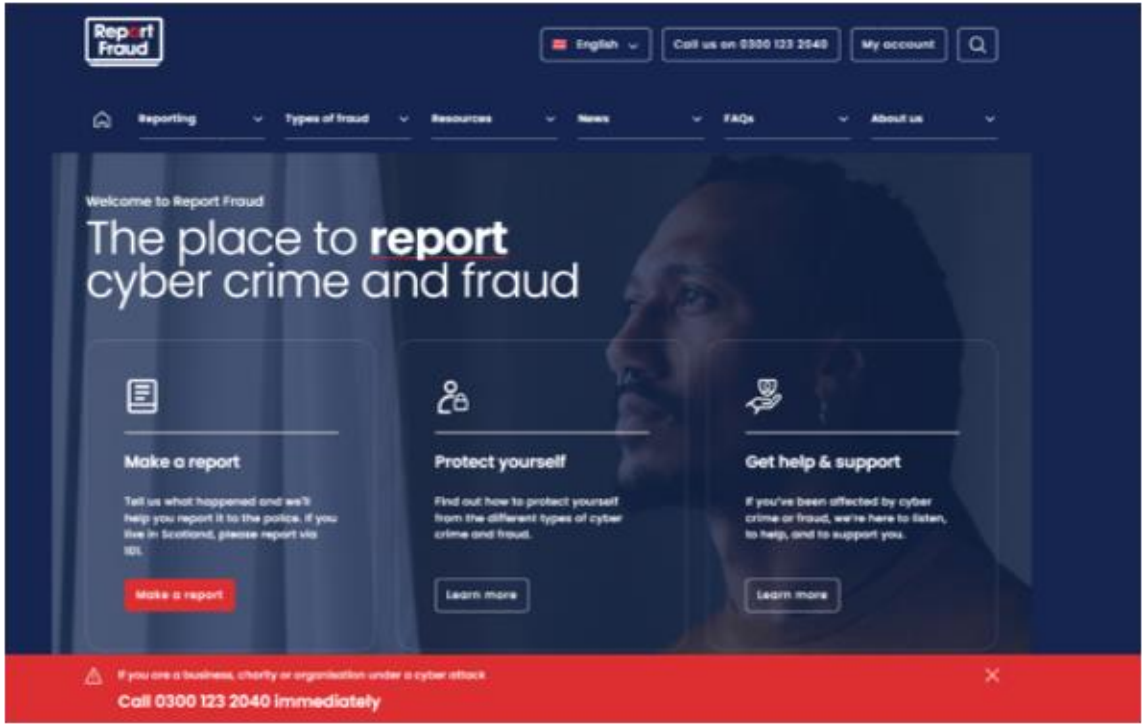
Report Fraud

CITY OF LONDON POLICE

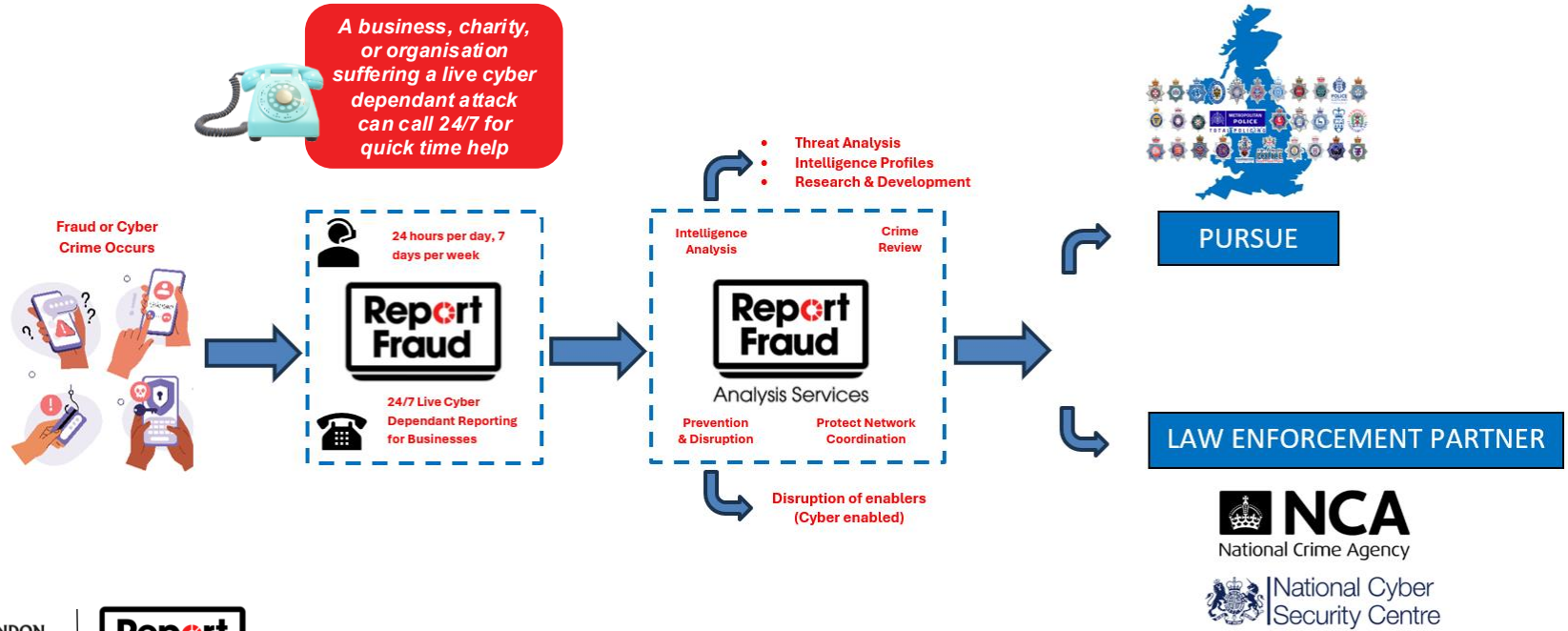
Report Fraud

Tell the police about cyber crime and fraud
reportfraud.police.uk or call 0300 123 2040

EVERY REPORT COUNTS



Reporting Cyber Crime and Fraud and Live Cyber Reporting



CITY OF LONDON POLICE | Report Fraud


Report
Fraud

5

Services for UK Businesses

Report Fraud

CITY OF LONDON POLICE

Protect Services available for Businesses

- The Protect Network – Regional Organised Crime Units (ROCUs)
- Police Cyber Alarm (PCA)
- Cyber Resilience Centres (CRCs)
- National Cyber Resilience Centre (NCSC)
- Cyber Essentials / Cyber Essentials Plus
- Stop! Think Fraud

Regional Organised Crime Units (ROCUs)

The policing Protect network spans across England, Wales, Northern Ireland, and Scotland.

In each region and local force there is a Protect team who focus on raising awareness around cyber crime and fraud through education and community engagements.

They also offer staff training at all levels of an organisation and team building exercises to better prepare the organisation should a cyber attack happen.

https://www.rocu.police.uk/our-national-network

POLICE CYBERALARM

Police Cyber Alarm is a free cyber threat detection tool funded by the Home Office and managed by the National Police Cybercrime Team.

It helps identify malicious external activity against a members' network through monitoring and vulnerability scanning.

https://www.cyberalarm.police.uk

NPCC
National Police Chiefs' Council

THE CYBER RESILIENCE CENTRE NETWORK

Scan to find your regional centre

There are 9 regional CRCs in England and Wales that make up The CRC Network.

The CRC Network is a strategic collaboration between police, government, private sector and academia to help strengthen cyber resilience across micros, small and medium-sized enterprises and third sector organisations to protect the UK economy.

CRC Services

Cyber Resilience Centres help businesses and third-sector organisations become more secure through knowledge sharing and signposting to trusted guidance.

- Membership is free and starts SMEs on a 16-part journey towards better cyber resilience
- Guiding them to trusted resources
- Encouraging them to adopt Cyber Essentials as a minimum standard
- Helping them protect themselves and those in their supply chains

National Cyber Security Centre
a part of GCHQ

CYBER ESSENTIALS

CYBER ESSENTIALS PLUS

CRC Services

- 1-2-1 cyber discussion
- Regional threat alerts
- Monthly newsletter
- Invites to webinars and business networking events
- Access to fully funded technical services provided by Cyber PATH

Cyber PATH Services

- Security Awareness Training
- First Step Web Assessment
- Full Web Application Assessment
- Internal Vulnerability Assessment
- External Vulnerability Assessment
- Business Continuity Review
- Security Policy Review
- Internet Discovery

The National Cyber Security Centre (NCSC) are the leading Government body in the UK for cyber crime. There are a range of services they offer to support businesses, from sole traders to large businesses and the public sector:

- Management guides
- Training for staff
- Cyber Essentials
- Exercise in a Box

National Cyber Security Centre

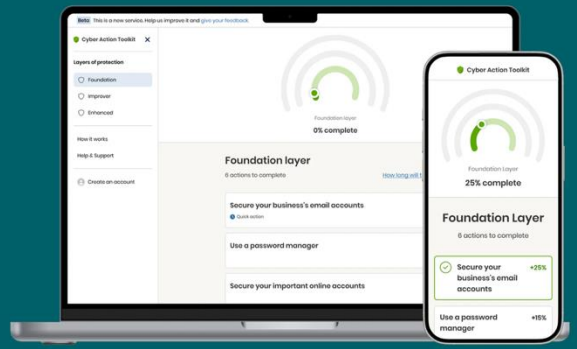
- Cyber Action Toolkit
- Mail/Web Check
- Supply Chain guide
- Early Warning Checker
- Cyber Security product assurance checker
- Cyber Governance resources and board member training

NCSC Reporting

NCSC also offers guidance on how to report cyber crime

https://www.ncsc.gov.uk/campaigns/cyber-resilience

National Cyber Security Centre



https://cybertoolkit.service.ncsc.gov.uk

Cyber Action Toolkit

The Cyber Action Toolkit is a free resource that provides clear, bite-size actions to help protect your business.

The tool is primarily aimed towards **small businesses**.

ACD

Active Cyber Defence services are a range of **free services** and tools offered by NCSC to eligible organisations.

This includes:

- Self-service checks: A range of services that guide you through various checks.
- Detections deployed by organisations: Eligible organisations integrate the offered services into their environment for protection and detection
- Disruption services

www.ncsc.gov.uk/section/active-cyber-defence/services

Cyber Essentials

Cyber Essentials is the minimum standard of cyber security recommended by the Government for organisations of all sizes.

Developed by the experts at the NCSC, the certification scheme is aligned to five technical controls designed to prevent the most common internet based cyber security threats.

iasme

https://iasme.co.uk/cyber-essentials/

03300 882 752

National Cyber Security Centre

Cyber Essentials Plus

The verified self-assessment questionnaire of Cyber Essentials is a prerequisite to Cyber Essentials Plus.

Although based on the same technical requirements, Cyber Essentials Plus includes a technical audit of your IT systems to verify that the controls are in place. In this way, it gives more assurance that you are complying with the scheme.

The audit covers a representative set of user devices, all internet gateways, and all servers with services accessible to the internet.

Why Cyber Essentials?

Cyber criminals can find your business anywhere. No matter your business' size or location, cyber attacks are no longer a question of 'if' but 'when'.

The good news is that most cyber-attacks are basic in nature - the digital equivalent of a thief trying your front door to see if it's unlocked.

Cyber Essentials helps ensure your door is locked shut, keeping your digital assets and data safe.

CYBER ESSENTIALS PLUS

Cyber Essentials Plus

- **SAME** scope as VSA.
- Assessor undertakes a remote or site visit.
- Technical audit of IT systems.
- CE questionnaire response used to plan the audit.
- External vulnerability scan is performed.
- Assessor provides feedback.

CYBER ESSENTIALS

Cyber Essentials Verified Self-Assessment

- Customer completes CE questionnaire on Pervade.
- Assessor marks assessment on the Pervade online platform.
- Assessor provides feedback.

www.ncsc.gov.uk/cyberessentials/resources

STOP! THINK FRAUD

Giving you the knowledge and tools you need to stay ahead of scams.

The UK Government has an ongoing campaign to raise awareness around cyber crime and fraud. Here they offer advice to businesses:

stopthinkfraud.campaign.gov.uk/protecting-your-business

The Home Office – Stop! Think Fraud

Any Questions?

Annette.West@cityoflondon.police.uk
Sarah.Bannon@cityoflondon.police.uk

Report Fraud | City of London Police

For general enquiries to Report Fraud (without submitting a report) visit:
https://reporting.reportfraud.police.uk/make-enquiry/