



**NCA**

National Crime Agency

# **National Cyber Crime Unit**

# NCA Vision

Message from Keith Bristow

“Protecting the public: leading our fight against serious and organised crime”

Working with our partners will be critical to the success of the agency and it will be our combined efforts, working to protect the public, that will have a real impact.

**Lead, Support, Co-ordinate**

# Office for National Statistics

In 2013, 36 million adults (73%) in Great Britain accessed the Internet every day, 20 million more than in 2006, when directly comparable records began.

Access to the Internet using a mobile phone more than doubled between 2010 and 2013, from 24% to 53%.

In 2013, 72% of all adults bought goods or services online, up from 53% in 2008.

In Great Britain, 21 million households (83%) had Internet access in 2013.

Broadband Internet connections using fibre optic or cable were used by 42% of households, up from 30% in 2012

Release Date: 08 August 2013

17 February 2011 Last updated at 11:49

784

Share



# UK cyber crime costs £27bn a year - government report

**Cyber crime costs the UK economy £27bn a year, the government has said.**

**The figures, published for the first time,** are a mid-range estimate and the real cost could be much higher.

They are made up of £21bn of costs to businesses, £2.2bn to government and £3.1bn to citizens.

Security minister Baroness Neville-Jones said the government was determined to work with industry to tackle cyber crime.

At the moment, cyber criminals are "fearless because they do not think they will be caught", she said in a briefing in central London.



Cyber crime is seen as a growing problem

---

## Related Stories

---

**UK opts in to EU cyber-crime plan**

**Cyber attacks 'are acts**

# Measuring the Cost of Cybercrime

Ross Anderson, Cambridge University  
Michael Levi, Cardiff University

## Cyber Crime

- \$97M Fake Antivirus
- \$10M↑ Stranded Traveler
- \$200M↑ Fake Escrow
- \$1,000M↑ Advanced Fee
- \$370M↑ Online Banking Fraud: Malware
- \$320M≈ Online Banking Fraud: Phishing

## Cyber Defense

- \$1,000M≈ Bank Countermeasures
- \$3,400M Antivirus
- \$40M≈ ISP Cleanup
- \$1,000M≈ Patching Vulnerabilities
- \$10,000M≈ User Cleanup
- \$10,000M≈ Business Security
- \$400M Law Enforcement

↑Likely an underestimate

≈ High uncertainty



Department  
for Business  
Innovation & Skills

**£450k -** is the average cost to a large organisation of its worst security breach of the year

**£35k -** is the average cost to a small business of its worst security breach of the year

**78%** of large organisations were attacked by an unauthorised outsider in the last year (up from 73% a year ago)

**39%** of large organisations were hit by denial-of-service attacks in the last year (up from 30% a year ago)

**20%** of large organisations detected that outsiders had successfully penetrated their network in the last year (up from 15% a year ago)

**14%** of large organisations know that outsiders have stolen their intellectual property or confidential data in the last year (up from 12% a year ago)

**2013 INFORMATION SECURITY BREACHES SURVEY**

Technical Report

Survey conducted by

**63%** of small businesses were attacked by an unauthorised outsider in the last year (up from 41% a year ago)

**23%** of small businesses were hit by denial-of-service attacks in the last year (up from 15% a year ago)

**15%** of small businesses detected that outsiders had successfully penetrated their network in the last year (up from 7% a year ago)

**9%** of small businesses know that outsiders have stolen their intellectual property or confidential data in the last year (up from 4% a year ago)

# What is cyber crime? – Serious and Organised Crime Strategy

Cyber crime describes two distinct, but closely related, criminal activities:

- **Cyber-dependent** crimes can only be committed using computers, computer networks or other forms of information communication technology (ICT). They include the creation and spread of malware for financial gain, hacking to steal important personal or industry data and denial of service attacks to cause reputational damage.
- **Cyber-enabled crimes** (such as fraud, the purchasing of illegal drugs & child sexual exploitation) can be conducted on or offline, but online may take place at unprecedented scale and speed.

<https://www.gov.uk/government/publications/serious-organised-crime-strategy>

Published 7<sup>th</sup> October 2013

# The Computer Misuse Act 1990

**Section 1** contains the basic '**hacking**' offence of gaining unauthorised access to any program or data held in a computer.

**Section 2** makes it an offence to commit a Section 1 offence with a view to commit, or facilitate the commission of, a further offence i.e. fraud

**Section 3** contains the offence of doing any unauthorised act in relation to a computer with intent:

- to impair the operation of any computer; or
- to prevent or hinder access to any program or data held in any computer; or
- to impair the operation of any such program or the reliability of such data;
- to enable any of the things to be done.

**Section 3A** – making, supplying or obtaining articles for use in S1 or 3

# Cybercrime-as-a-Service

**CHEAP PROFESSIONAL DDOS SERVICE**

Cheap Professional DDOS Service  
Trusted  
Strong/Fast Service  
Takes down Large Website/Forum/Game Servers etc.  
No time limit

**PRICE**

1 - 4 hours / 2\$ per hour  
5 - 24 hours / 4\$ per hour  
24 - 72 hours / 5\$ per hour  
1 month / 1000\$ fix price

**PAYMENT ACCEPTED**

Paypal ( Verified users only )  
Liberty Reserve  
Western Union  
MoneyBookers

Table 2. Prices for stolen credit card numbers.

Dumps	Estimate of Prices (without PIN, with PIN, PIN and good balance)									
	US		EU		CA, AU		Asia			
Visa Classic	\$15	\$80	\$40	\$150	\$25	\$150	\$50	\$150		
Master Card Standard		\$90		\$140		\$150		\$140		
Visa Gold/Premier	\$25	\$100	\$200	\$45	\$160	\$250	\$30	\$160	\$55	\$150
Visa Platinum	\$30	\$110		\$50	\$170		\$35	\$170	\$60	\$170
Business/Corporate	\$40	\$130		\$60	\$170		\$45	\$175	\$70	\$170
Purchasing/Signature	\$50	\$120		\$70			\$55		\$80	
Infinite				\$130	\$190		\$60	\$200		\$190
Master Card World		\$140								
AMEX	\$40			\$60			\$45		\$70	
AMEX Gold	\$70			\$90			\$75		\$100	
AMEX Platinum	\$50									

Table 1. Prices for zero-day vulnerabilities.

Adobe Reader	\$5,000–\$30,000
Mac OS X	\$20,000–\$50,000
Android	\$30,000–\$60,000
Flash or Java Browser Plug-ins	\$40,000–\$100,000
Microsoft Word	\$50,000–\$100,000
Windows	\$60,000–\$120,000
Firefox or Safari	\$60,000–\$150,000
Chrome or Internet Explorer	\$80,000–\$200,000
IOS	\$100,000–\$250,000

Cracking Order Faqs Contact

**Email Password Cracking made easy..!!**

Request an E-mail Password :-  
Fill in the below form to the best of your knowledge. Make sure that the email addresses are entered correctly. Once submitted, check your email for a confirmation mail. Add our email address(es) in your address-book, to prevent our emails and the proofs landing in bulk folder. Once you verify the order by clicking on the confirmation link sent to you, we will process your order.

Your Name:

Your Email Address:

Confirm your Email Address:

Your Country:

Most Urgent  Urgent  Just do it whenever you can

Victim Name:

Victim Email Address:

Confirm Victim Email Address:

Victim Country:

Victim Language:

Optional Information :-

Log in

**LIVE CHAT**  
Offline now. Leave a message.  
Send Here

Home > Smtp Relay Server > Smtp Relay Server for 30 000 000 emails

**SMTP RELAY SERVER FOR 30 000 000 EMAILS**

Smtp Relay Server for 30 000 000 emails for the one month

**PRICE LOWERED!**  
**\$13,340.25 tax incl.**  
\$44,822.50 tax incl.  
(price reduced by 10 %)

Quantity:

Availability: 999 items in stock

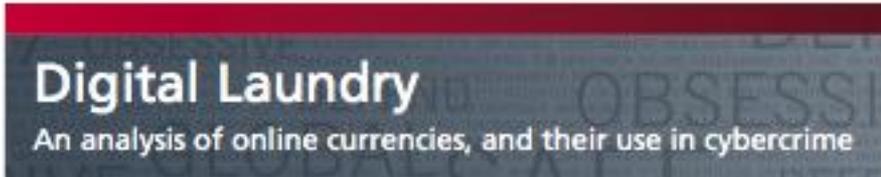
**PayPal**  
Click here to pay

Categories:  
2012 Business Email List  
2012 Country Email List  
2012 Domain Email Lists  
2012 Email List  
2012 General Global Email Lists  
2012 Men's Email Lists  
2012 Targeted Email List  
2012 Woman Email List  
Discounted Price  
Email Marketing Campaigns  
Mass Email Software  
Smtp Relay Server

Diagram: Sender's SMTP Server -> Recipient's Backup SMTP Server #2 -> Recipient's SMTP Server #1

Figure 10. This spam service offers support, just like many legitimate online offers.

# Virtual Currencies



WebMoney    Perfect Money

Bitcoin    UKASH    e-gold

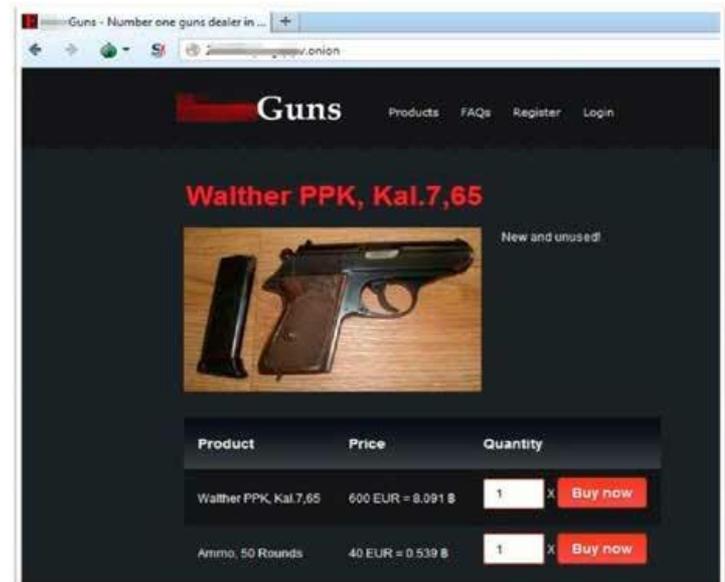
Liberty Reserve

Bitcoin address for receiving payments into this wallet:  
1QHbyiqAHo[redacted]Aw16iTv6  
[ Show QR code for Bitcoin address ] [ Show QR code for unique link of this Instawallet ]

**Send payment**

Bitcoin address:

Amount:  BTC  Use green address (What is this?)



Product	Price	Quantity
Walther PPK, Kal.7,65	600 EUR = 8.091 \$	<input type="text" value="1"/> <input type="button" value="x"/> <input type="button" value="Buy now"/>
Ammo, 50 Rounds	40 EUR = 0.539 \$	<input type="text" value="1"/> <input type="button" value="x"/> <input type="button" value="Buy now"/>

# NCA Structure

DG Keith Bristow  
DDG Phil Gormley

CEOP

Organised  
Crime  
Command

Economic  
Crime  
Command

Borders

NCCU

Intelligence Hub

# NCCU Mission

The aim of the NCCU is to:

- collaborate with partners to fight crime
- protect the public and reduce harm to the UK from cyber and cyber-enabled crime
- provide a specialised investigative response, nationally and internationally, to the most serious incidents of cyber crime
- work to eliminate criminal opportunities and create a hostile environment for cyber criminals
- assist law enforcement to tackle cyber and cyber-enabled crime
- support a step-change in UK law enforcement's mainstream cyber capabilities.

# NCCU Structure

Strategy, Performance &  
Coordination

Cyber Ops

Ops Support

Partnerships  
and  
Expertise

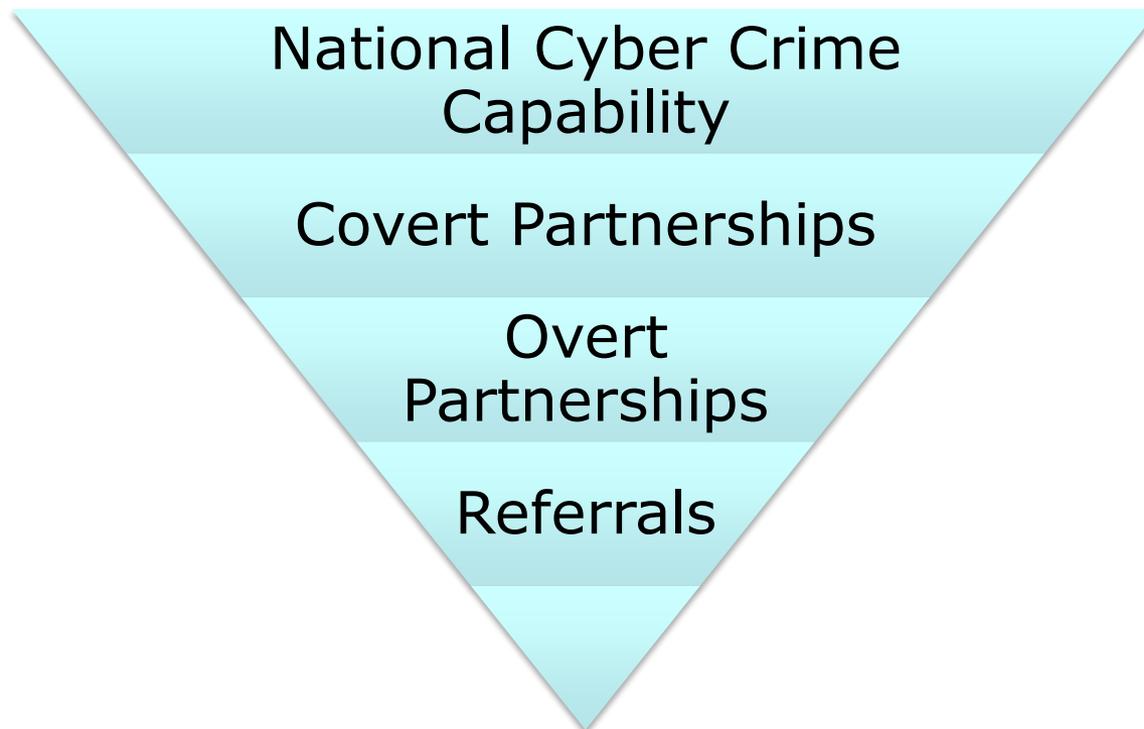
# Cyber Operations



# Operational Support

- Operational investigative support
  - Technical
  - Intelligence
  - Financial
  - Enforcement
- Cyber international liaison

# Partnership & Expertise



Prevention, disruption, enrichment of  
the intelligence picture & response

# Challenges

- The internet
- Multi-jurisdictional
- Legislation
- Working with industry
- Skills in policing
- Competing priorities



# Action Fraud

and internet crime reporting centre

**Action Fraud**  
Report Fraud & Internet Crime  
**0300 123 2040**

[Home](#) [About us](#) [Report it](#) [Types of fraud](#) [Support & prevention](#) [Resources](#) [News & alerts](#)

## Action Fraud is the UK's national fraud and internet crime reporting centre

We provide a central point of contact for information about **fraud** and **financially motivated internet crime**. If you've been scammed, ripped off or conned, there is something you can do about it. **Report fraud** to us and receive a **police crime reference number**.

*Action Fraud is not an emergency service - dial 999 if you are in immediate danger.*

We use cookies to ensure that we give you the best experience on our website. You can [disable cookies](#) at any time.

Skip to main content

Search

received by older and vulnerable residents in Scotland are nuisance calls [9 September 2013]

### Who reports frauds to us

Frauds committed in the UK will be reported to Action Fraud; from individuals up to larger corporations and financial institutions. Find out more by clicking on an icon below.

Why you should report fraud >>



Individuals



Police officers



Charities



Small Businesses



Large Corporations

### Working together

The National Fraud Authority works together with the City Of London Police to deliver Action Fraud



### Our Partners

We work closely with our partners in government and the police to run the Action Fraud reporting service for you.



### Latest News



#### Bank card fraudsters jailed

Three bank card fraudsters were given a total of 7 years sentence for theft, following an operation led by the banking industry-sponsored Dedicated Cheque and Plastic Crime Unit (DCPCU) [10 September 2013]



#### Nuisance calls make up 40% of calls to elderly and vulnerable

A trading standards investigation has revealed that about 40% of the phone calls received by older and vulnerable residents in Scotland are nuisance calls [9 September 2013]

### Chat

Online advisor  
**LIVE CHAT**

### Action Fraud on Twitter

**Crimestoppers**  
@CrimestoppersUK

**Crimestoppers**  
@CrimestoppersUK

Fine wine fraudsters jailed for conning elderly investors via @Crime\_Telegraph bit.ly/19Gopy0 #befraudaware bit.ly/1eCSFxx

Retweeted by Action Fraud  
Show Summary

**Action Fraud**  
@actionfrauduk

Would you like plastic money? Banknotes made of polymer and are reportedly more secure against fraud [bbc.in/19GFgB1](http://bbc.in/19GFgB1)  
Expand

### Like us on Facebook

**Action Fraud**  
Like

3,948 people like Action Fraud.



Facebook social plugin

[http://www.apccs.police.uk/fileUploads/APCC\\_Group\\_Emails/130408\\_NPR\\_Final\\_Document\\_2.pdf](http://www.apccs.police.uk/fileUploads/APCC_Group_Emails/130408_NPR_Final_Document_2.pdf)



# National Policing Requirement

## Chapter 7

### National Requirements for Large-Scale Cyber Incidents

#### 7.1 Overview

7.1.1 Cyber security is defined as one of four top priorities for UK national security<sup>64</sup>. The term 'cyber attack' covers anything from small-scale email scams to sophisticated large-scale attacks driven by diverse political and economic motives.

7.1.2 The National Security Risk Assessment<sup>65</sup> identifies a large-scale cyber incident and the risk of a hostile cyber attack by other states as Tier 1 risks. It is important to note that a cyber incident may not necessarily result from a criminal attack but could be caused by a technological issue or failure.

7.1.3 The UK Cyber Security Strategy<sup>66</sup> outlines these objectives for the UK:

- **tackle** cyber crime and be one of the most **secure** places in the world to do business
- be more **resilient** to cyber attacks and able to **protect** interests in cyberspace
- help **shape** an open, stable and vibrant cyberspace which the UK public can use safely
- have cross-cutting **knowledge and skills** to underpin the achievement of these objectives.

2012



Inspecting policing  
in the public interest

## Strategic Policing Requirement inspection

Terms of Reference

<http://www.hmic.gov.uk/publication/strategic-policing-requirement-inspection-terms-of-reference/>

Search for Roles

Log-in: Username

- PPF Home
- About the PPF
- National Roles
- Personal Qualities



PPF Home > Search

## Search the Policing Professional Framework (PPF)

Search for:

Match:  Any words  All words  Exact phrase

### Results for 'cyber'

8 results found.

- [Cyber Infrastructure Officer](#)  
Police Officer Role  
National Role  
To develop and maintain tactical and strategic relationships with industry and other cyber-crime related partners. To design and implement methods of abuse prevention and...
- [Cyber Intelligence Analyst](#)  
Police Staff Role  
National Role  
... and reducing crime and disorder. This is carried out in relation to cyber crime as defined by the Home Office and the National Strategy.
- [Cyber Investigator \(DI\)](#)  
Police Officer Role  
National Role  
... detectives and police staff concerned in the investigation of serious and organised Cyber Crime. This is carried out in relation to cyber crime as...
- [Cyber Investigator \(DC\)](#)  
Police Officer Role  
National Role  
... which is admissible in Court. This is carried out in relation to cyber crime as defined by the Home Office and the National Strategy.
- [Cyber Investigator \(DS\)](#)  
Police Officer Role  
National Role  
... and serious internet based criminality. This is carried out in relation to cyber crime as defined by the Home Office and the National Strategy.
- [Cyber Intelligence Researcher](#)  
Police Staff Role  
National Role  
To service intelligence requirements in support of unit investigations in relation to cyber crime as defined by the Home Office and the National Strategy.
- [Cyber Intelligence Development Supervisor](#)  
Police Officer Role  
National Role  
... involvement or otherwise in criminal activity. This is carried out in relation to cyber crime as defined by the Home Office and the National Strategy.
- [Cyber Intelligence Development Officer](#)  
Police Officer Role  
National Role  
... operations to establish involvement or otherwise in criminal activity in relation to cyber crime as defined by the Home Office and the National Strategy.

Search for Roles

Log-in: Username

- PPF Home
- About the PPF
- National Roles
- Personal Qualities



PPF Home > National Roles > Police Officer Ranks > Constable > Cyber Investigator (DC)

## National Roles

### National Role

#### About this National Role

Type	Police Officer
Rank / Level	Constable
Role Type	Role
Updated	12th July 2013

- 
- 
- 

## Policing Professional Framework (PPF)

### Cyber Investigator (DC)

To carry out this role you must be a competent [Detective Constable](#).

To conduct investigations and operations into the most serious incidents of network based organised criminal activity; to detect hi-tech crime, gather and distribute relevant and quality intelligence; to provide technical advice and assistance to officers engaged in the investigation of hi-tech crime; to produce evidence in a form which is admissible in Court. This is carried out in relation to cyber crime as defined by the Home Office and the National Strategy.

A Cyber Investigator (DC) must be able to

- Identify and secure electronic evidence sources
- Seize and record electronic evidence sources
- Capture and preserve electronic evidence
- Investigate electronic evidence
- Evaluate and report electronic evidence
- Conduct Open Source Internet investigations
- Conduct network investigations
- Identify and deal with threat and areas of vulnerability
- Recover technical equipment
- Health and Safety in ICT and Contact Centres at level 1

## Personal Qualities

- Decision making** [ view ]
- Leadership** [ view ]
- Professionalism** [ view ]
- Public service** [ view ]
- Working with others** [ view ]

## Associated Qualifications, Accreditation and Learning Programmes

### Phase 1 - Suggested Basic Training

Training covering the following areas

- Open Source
- Advanced Internet Research
- Core Skills in Network Investigation
- Core Skills in Digital Investigation
- Access Data Forensic Toolkit
- How to conduct 'active file review' from a forensic image

# Reference documents

- **ACPO Managers Guide** - Good Practice and Advice Guide for Managers of e-Crime Investigation
- **ACPO Good Practice Guide** for Digital Evidence *March 2012*
- **National Policing Requirement** for the Strategic Policing Requirement - Chapter 7 National Requirements for Large Scale Cyber Incidents
- **Serious and Organised Crime Strategy** *October 2013*
- **10 Steps to Cyber Security**
- **Small businesses: What you need to know about cyber security** *2013*
- [www.getsafeonline.org](http://www.getsafeonline.org)
- [www.actionfraud.police.uk](http://www.actionfraud.police.uk)
- [www.ecrimewales.com](http://www.ecrimewales.com)

# What works

- A standards based approach to IT Hygiene, including a response to witting or unwitting employees that cause harm
- Shared intelligence and threat data, by sector or trade body
- Understanding the threat picture and your capability to respond, including protecting and backing up sensitive data
- Cross Government & industry collaboration on the threat, intelligence, response, mitigation and recovery
- Exercising the disaster response and business continuity
- Fast time incident response, whilst crime is in action, with a live forensics capability
- Education on business continuity, prevention, mitigation & disaster recovery (GSoL, CESG, CPNI, CISP)
- Being cognisant of emerging & future technologies