

Our Ref: IM-FOI-2015-1150



Sir Stephen House QPM  
Chief Constable

## **FREEDOM OF INFORMATION (SCOTLAND) ACT 2002**

I refer to your recent request for information which has been handled in accordance with the Freedom of Information (Scotland) Act 2002.

For ease of reference, your request is replicated below together with the response.

- 1. What is Police Scotland's definition of a cyber-crime incident?**
- 2. What is Police Scotland's definition of a cyber-enabled crime?**
- 3. What is Police Scotland's definition of a cyber-dependent crime?**
- 4. What is Police Scotland's definition of a cyber-facilitated crime?**

*For ease, Q1 – 4 have been answered together.*

Cybercrimes can be defined in two ways:

Pure Cybercrimes (or computer-dependent crimes) are where a criminal act can only be committed through the use of computers or other ICT devices. In these cases the devices are both the tool for committing the crime and target of the crime. For instance, the harvesting of online bank account details using malware, the hacking of a website through SQL injection, hacking of networks to steal sensitive data or distributed denial of service attacks on websites or infrastructure.

Cyber-enabled crimes are those that may be committed without ICT devices, but are changed by use of ICT in terms of scale and reach. This can comprise a wide range of criminal activities, including, but not limited to, online fraud, online theft, online sexual offending and where the devices are used to organise or arrange crimes.

### **5. Which part of Police Scotland has the lead in tackling cyber crime offences and who within Police Scotland has responsibility for this?**

The investigation of Cybercrime is not confined to a specific number of police officers within Police Scotland. The investigation will be led by an officer of suitable rank and location based on the crime under investigation. Therefore, any one of our rank and file officers could be dedicated to lead such an investigation. Support to such investigations is provided from a wide range of departments within Police Scotland and where required, specialist police officers received training in specialist courses to include mobile forensics, computer forensics and network forensics.

### **6. Do Police Scotland receive cyber-crime reports directly or are reports of all cyber incidents received through Action Fraud?**

Police Scotland is involved in the reactive and proactive policing of the internet to include many and various forms of online offending. These can include acquisitive crimes such as online fraud, online theft and phishing, child abuse involving paedophilic criminality, the distribution of malware such as ransomware cases and the investigation of digital attacks on computer infrastructures such as distributed denial of service (DDoS) attacks and system interference.

**7. How many 'cyber-enabled' crimes have been reported to Police Scotland directly from 1 January 2014 to 31 December 2014? Of these, how many were a) investigated and b) resolved?**

*For ease I have answered Q7 and 9 together*

**9. How many 'cyber-dependent' crimes have been reported to Police Scotland directly from 1 January 2014 to 31 December 2014? Of these, how many were a) investigated and b) resolved?**

I have considered your request and am afraid that I am unable to provide a response, as it would prove too costly to do so within the context of the fee regulations. As you may be aware the current cost threshold is £600 and I estimate that it would cost well in excess of this amount to process your request.

As such, and in terms of Section 16(4) of the Freedom of Information (Scotland) Act 2002 where Section 12(1) of the Act (Excessive Cost of Compliance) has been applied, this represents a refusal notice for the information sought.

To explain, Police Scotland operates a number of crime recording systems. Whilst robust statistical analysis can be made of the data held on each of our systems, they are not, at present, designed to enable the retrieval of the highly specific information as per your request. The only way to provide you with this information in an accurate and consistent manner would be to individually examine each crime report created on these systems in 2014 as outwith the obvious 'cyber crimes' such as Computer Misuse Act 1990 offences, many crimes including, but not exclusively, Fraud, Theft and Sexual Offences are recorded as such but may feature a 'Cyber-enabled' or 'Cyber-dependant' aspect.

**8. How many 'cyber-enabled' crimes have been reported to Police Scotland via Action Fraud from 1 January 2014 to 31 December 2014? Of these, how many were a) investigated and b) resolved?**

*For ease I have answered Q8 and 10 together*

**10. How many 'cyber-dependent' crimes have been reported to Police Scotland via Action Fraud from 1 January 2014 to 31 December 2014? Of these, how many were a) investigated and b) resolved?**

I have considered your request and am afraid that I am unable to provide a response, as it would prove too costly to do so within the context of the fee regulations. As you may be aware the current cost threshold is £600 and I estimate that it would cost well in excess of this amount to process your request.

As such, and in terms of Section 16(4) of the Freedom of Information (Scotland) Act 2002 where Section 12(1) of the Act (Excessive Cost of Compliance) has been applied, this represents a refusal notice for the information sought.

To explain, Police Scotland operates a number of crime recording systems. Whilst robust statistical analysis can be made of the data held on each of our systems, they are not, at present, designed to enable the retrieval of the highly specific information as per your request. The only way to provide you with this information in an accurate and consistent manner would be to individually examine each crime report created on these systems in 2014. For N Division, in 2014 alone this would entail examining over 25,000 such reports.

You may wish to make a further request directly to NFIB, City of London Police Headquarters, Guildhall Yard East, London EC2V 5AE.

**11. How many cyber-crime investigations conducted by Police Scotland from 1 January 2014 to 31 December 2014 have led to arrest? What percentage of the overall number of cyber crimes reported to Police Scotland over the same period was this?**

I would ask that you note that the police in Scotland have the power to arrest an individual where there is sufficient evidence to support a charge against them, for a common law crime or for a statutory offence where the statute empowers the police to arrest, without warrant, any person contravening its provisions. When a statute confers power to arrest any person contravening its provisions, this power should be exercised only if it is necessary in the interests of justice that the offender should be taken into custody. Where citation will prove equally effectual, arrests should not be made.

Therefore as arrests are not recorded in an easily retrievable format, the rationale set out above for the Section 12 cost exemption will also apply.

**12. How many cyber-crime investigations conducted by Police Scotland from 1 January 2014 to 31 December 2014 have led to prosecution? What percentage of the overall number of cyber crimes reported to Police Scotland over the same period was this?**

As explained in questions 7, 9 and 11 above Police Scotland are unable to provide figures regarding 'cyber-crime'. Notwithstanding the rationale described above, information regarding prosecutions is not held by Police Scotland and, as such you may wish to make this request directly to the FOI Officer, Scottish Court Service Headquarters, 1A Parliament Square, Edinburgh, EH1 1RF. Therefore under Section 17 of the Freedom of Information (Scotland) Act 2002 I must inform you that we do not hold the information you have requested.

**13. Is Police Scotland a member of the Cyber-Security Information Sharing Partnership (CiSP)?**

Police Scotland has been an active member of CiSP since June 2014.

**14. In addition to the specific questions above, could you please tell me what other initiatives Police Scotland are delivering, or exploring, to address the growing problem of low level, high volume cyber-crime?**

Police Scotland are fully committed to ongoing engagement with other Law Enforcement agencies, key partners in business, education, academia and the voluntary sector, delivering workshops and on line safety messages around all aspects of Cybercrime and in particular low level high volume Cybercrime.

Should you require any further assistance concerning this matter please contact me directly on 01463 720555 quoting the reference number given.

If you are not satisfied with the way in which your request has been dealt with, you are entitled in the first instance, and within 40 working days of receiving this response, to request a review of the decision. Should you wish to do so, contact details are; FOI Central Processing Unit, Police Scotland, Clyde Gateway, 2 French Street, Dalmarnock, G40 4EH - [foi@scotland.pnn.police.uk](mailto:foi@scotland.pnn.police.uk)

If you remain dissatisfied following the outcome of that review, you are thereafter entitled to apply to the Scottish Information Commissioner within six months for a decision. Contact details are; Office of the Scottish Information Commissioner, Kinburn Castle, Doubledykes Road, St Andrews, Fife, KY16 9DS - [enquiries@itspublicknowledge.info](mailto:enquiries@itspublicknowledge.info)

Should you wish to appeal against the Scottish Information Commissioner's decision, there is an appeal to the Court of Session on a point of law only.

Yours sincerely,

**Donna Quick**  
Information Management