Keeping People Safe

FREEDOM OF INFORMATION REQUEST

Request Number: F-2018-01621

Keyword: Organisational Information/Governance

Subject: Fraudulent Emails

Request and Answer:

Your request for information has now been considered. In respect of Section 1(1)(a) of the Act I can confirm that the Police Service of Northern Ireland does hold some information to which your request relates and this is being provided to you. PSNI is providing an NCND (Neither confirm nor deny) response in relation to Request 2, 4, 6 & 11. And this is explained further in the response below. We have also provided you with links to guidance issued by the Information Commissioner's Office which we have followed in responding to your request.

Under Section 11 of the FOIA applicants have the right to express a preference for the summary of information that is acceptable to the applicant. However, subject to subsection (1) a public authority may comply with a request by communicating information by any means which are reasonable in the circumstances. There is no requirement to respond to this request in its questionnaire form. Information is provided in the format below as this is the usual manner in which PSNI release information under FOI.

Request 1
What percentage of emails that your organisation receives are fraudulent – i.e. phishing messages, BEC (business email compromise) attacks, CEO Fraud, malware laden, etc.
• Please indicate as a percentage
• Don't Track

Answer
PSNI receive on average, 58,000 emails per week and 7.1 % identified as fraudulent.

Request 3
Has your organisation suffered financial loss in the last 12 months as a direct result of a faked email message being received that tricked an employee into sending money via wire transfer
• Yes
• No
If yes, please state how much was lost (if fallen victim more than once, please provide total amount given to scammers)

Answer
The Freedom of Information Act requires PSNI to provide a response to a request for 'recorded' information which is held (s.1 FOIA). A question will not necessarily constitute a 'valid request' if it is

seeking a ‘yes’ or ‘no’ response unless it is already held in recorded information, if it is asking PSNI to speculate or if it seeks information which is not recorded.

Further information on what constitutes a valid request can be found on the Information Commissioner’s Office website:

https://ico.org.uk/media/for-organisations/documents/1164/recognising-a-request-made-under-the-foia.pdf

Request 5
Do you use the domain-based message authentication, reporting and conformance protocol (DMARC) to block fake emails being spoofed to appear as if they have been sent by your company/organisation:
• Yes
• No
• Don’t know

Answer
Yes.

Request 7
Do you publicise externally how a member of the public can check an email communication with your organisation to determine if it is fake?
• Yes
• No
If yes, how many reports have you received in the last 6 months of fake/phishing messages.
• Don’t Track

Answer
PSNI do not publicise externally how a member of the public can check and email communication with PSNI to determine if it is fake. Members of the public can use Action Fraud to report concerns of this nature.

Request 8
Do you publicise internally how a member of your workforce (including third party suppliers) can check an email communication with your IT/Security team to determine if it is fake?
• Yes
• No
If yes, how many reports have you received in the last 6 months of fake/phishing messages:
• from internal workforce
• from third party suppliers
• from both internal and third party suppliers as don’t differentiate between senders
• Don’t Track

Answer
No, PSNI do not publicise internally how a member of our workforce can check an email communication to determine if it is fake.

Request 9
Do you provide a report button within your email system for end users to report phishing emails?
• Yes
• No

Answer
No.

Request 10
Does your organisation have a SOC (Security Operations Centre) or IT security team?

- Yes
- No

Answer
Yes.

In accordance with the Act, this letter represents a Refusal Notice for part of this request. The Police Service of Northern Ireland can neither confirm nor deny that it holds the information you have requested in relation to Request 2, 4, 6, & 11.

Request 2
What is the most common type of fraudulent email/cyber-attack that your organisation receives?
• CEO fraud – this is when someone sends an email impersonating a senior company executive asking an employee to make payments for goods or services into a fraudulent bank account
• Fraudulent transaction requests – fraudsters send invoices for payment of goods or services as if from a legitimate organisation
• Credential theft – fraudsters send messages trying to get users to divulge their username and password or other sensitive information
• Ransomware
• Other
• Don't Track

Request 4
Has your organisation had a device/system infected by ransomware in the last 12 months that was delivered via email:
• Yes – once
• Yes – more than once
• We were infected by ransomware but the source wasn't traced
• Never
NB: If you have answered yes, please answer the following questions for each separate ransomware infection (if numerous devices were infected at the same time, this counts as one incident)
How long were systems affected.
Did you pay the ransom:
- Yes
- No

If yes, how much was paid.
Did the criminals provide the information/program needed to restore systems:
- Yes
- No

Request 6
Are you aware if your organisation/brand has ever been 'spoofed' and used by scammers to send emails trying to trick people
- Yes – before we started using DMARC
- Yes – after we started using DMARC
- Yes – but not sure if it was before or after using DMARC
- Never
- Don't Track

If yes, please state how many separate incidents of your organisation/brand being spoofed that you know of:
before we started using DMARC

after we started using DMARC

Request 11
Do you have a secure email gateway?
- Yes
- No
- Don't know

Answer
Section 1 of the Freedom of Information Act 2000 (FOIA) places two duties on public authorities. Unless exemptions apply, the first duty at Section 1(1)(a) is to confirm or deny whether the information specified in the request is held. The second duty at Section 1(1)(b) is to disclose information that has been confirmed as being held.

Where exemptions are relied upon Section 17(1) of FOIA requires that we provide the applicant with a notice which

a) states that fact,
b) specifies the exemption(s) in question and
c) states (if that would not otherwise be apparent) why the exemption applies.

PSNI can neither confirm nor deny that information is held relevant to your request as the duty in Section 1 (1) (a) of the Freedom of Information Act 2000 does not apply by virtue of the following exemptions:

Section 24(2) - National Security - The duty to confirm or deny does not arise if, or to the extent that, exemption from section 1(1)(a) is required for the purpose of safeguarding national security.

Section 31(3) - Law Enforcement - The duty to confirm or deny does not arise if, or to the extent that, compliance with section 1(1)(a) would, or would be likely to, prejudice any of the matters mentioned in subsection (1).

The full text of exemptions can be found at www.legislation.gov.uk and further guidance on how they operate can be located on the Information Commissioners Office website www.ico.org.uk.

'Neither Confirm nor Deny' (NCND)
There may be occasions when complying with the duty to confirm or deny under section 1(1) (a) would in itself disclose sensitive or potentially damaging information that falls under an exemption. In these circumstances, the Act allows a public authority to respond by refusing to confirm or deny whether it holds the requested information.

The decision to issue a 'neither confirm nor deny' response is not affected by whether we do or do not hold the information but relates to the consequences of confirming or denying the information is held. The starting point and main focus in most cases will be theoretical considerations about the consequences of confirming or denying that a particular type of information is held. The decision to neither confirm nor deny is separate from a decision not to disclose information and needs to be taken entirely on its own merits.

PSNI follow the Information Commissioner's Guidance in relation to 'NCND' and you may find it helpful to refer to this at the following link:

https://ico.org.uk/media/for-organisations/documents/1166/when_to_refuse_to_confirm_or_deny_section_1_foia.pdf

Sections 24 and 31 being prejudice based qualified exemptions there is a requirement to articulate the harm that would be caused in confirming or not whether information is held as well as considering

the public interest.

Harm in confirming or denying that information is held
To confirm or deny whether a cyber-crime has taken place or to provide information relating to fraudulent emails that allows for criminals to understand weaknesses within forces would identify vulnerable computer systems and provide actual knowledge or not that these incidents have taken place.

The release of information under Freedom of Information (FOI) is a release into the public domain and not just to the individual requesting the information. Once information is disclosed under FOI there is no control or limits as to who or how the information is shared with other individuals, therefore a release under FOI is considered a disclosure to the world in general.

In order to counter criminal and terrorist behaviour it is vital that the police and other agencies have the ability to work together, where necessary covertly, in order to obtain intelligence within current legislative frameworks to ensure the arrest and prosecution of offenders who commit or plan to commit acts of terrorism, whereby their modus operandi may involve criminal activities. In order to achieve this goal it is vitally important that information sharing takes place with other police forces and security bodies within the United Kingdom in order to support counter-terrorism measures in the fight to deprive terrorist networks of their ability to commit crime. To confirm or deny specific details of any breaches of information technology, security and vulnerabilities in technology would be extremely useful to those involved in terrorist activity as it would enable them to map vulnerable information security databases.

Public Interest

Factors Favouring Confirmation or Denial - Section 24 (2) National Security

The public are entitled to know how public funds are spent and how resources are distributed within an area of policing. To confirm where information security breaches have occurred or to highlight vulnerabilities would enable the general public to hold PSNI to account ensuring all such breaches are recorded and investigated appropriately. In the current financial climate of cuts and with the call for transparency of public spending this would enable improved public debate.

Factors Against Confirmation or Denial - Section 24 (2) National Security

Security measures are put in place to protect the community that we serve. As evidenced within the harm to confirm where specific breaches have occurred or vulnerable systems are in place would highlight to terrorists and individuals intent on carrying out criminal activities vulnerabilities within PSNI. Taking into account the current security climate within the United Kingdom, no information (such as the citing of an exemption which confirms information pertinent to this request is held or conversely, stating ‘no information held’) which may aid a terrorist should be disclosed. To what extent this information may aid a terrorist is unknown, but it is clear that it will have an impact on the forces ability to monitor terrorist activity. Irrespective of what information is or isn’t held, the public entrust the Police Service to make appropriate decisions with regard to their safety and protection and the only way of reducing risk is to be cautious with what is placed into the public domain. The cumulative effect of terrorists gathering information from various sources would be even more worrying when linked to other information gathered from various sources about terrorism. The more information disclosed over time will give a more detailed account of the tactical infrastructure of not only the force area but also the country as a whole. Any incident that results from such a disclosure would by default effect National Security.

Factors Favouring Confirmation or Denial – Section 31(3) Law Enforcement

Confirmation that information exists relevant to this request would lead to a better informed public

which may encourage individuals to provide intelligence in order to reduce such security breaches.

Factors Against Confirmation or Denial - Section 31(3) Law Enforcement

Confirmation or denial that information is held in this case would suggest PSNI take their responsibility to protect information and information systems from unauthorised access, destruction, etc., dismissively and inappropriately. The construction of a mosaic picture of vulnerable areas could also occur.

Decision
The points above highlight the merits of confirming or denying the requested information exists. The Police Service is charged with enforcing the law, preventing and detecting crime and protecting the communities we serve. As part of that policing purpose, information is gathered which can be highly sensitive relating to high profile investigative activity. Weakening the mechanisms used to monitor any type of criminal activity, and specifically terrorist activity would place the security of the country at an increased level of danger. In order to comply with statutory requirements and to meet NPCC expectation of the Police Service regarding the management of information security a national policy approved by the College of Policing titled National Policing Community Security Policy has been put in place. This policy has been constructed to ensure the delivery of core operational policing providing appropriate and consistent protection for the information assets of member organisations. A copy of this can be found at the below link:

http://library.college.police.uk/docs/APP-Community-Security-Policy-2014.pdf

Taking all these factors into consideration, I am satisfied that the exemptions outlined above are applicable to this request. It is for these reasons that the public interest must favour neither confirming nor denying that the requested information is held.

However, this should not be taken as conclusive evidence that the information you requested exists or does not exist.

If you have any queries regarding your request or the decision please do not hesitate to contact me on 028 9070 0164. When contacting the Freedom of Information Team, please quote the reference number listed at the beginning of this letter.

If you are dissatisfied in any way with the handling of your request, you have the right to request a review. You should do this as soon as possible or in any case within two months of the date of issue of this letter. In the event that you require a review to be undertaken, you can do so by writing to the Head of Freedom of Information, PSNI Headquarters, 65 Knock Road, Belfast, BT5 6LE or by emailing foi@psni.pnn.police.uk.

If following an internal review, carried out by an independent decision maker, you were to remain dissatisfied in any way with the handling of the request you may make a complaint, under Section 50 of the Freedom of Information Act, to the Information Commissioner's Office and ask that they investigate whether the PSNI has complied with the terms of the Freedom of Information Act. You can write to the Information Commissioner at Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF. In most circumstances the Information Commissioner will not investigate a complaint unless an internal review procedure has been carried out, however the Commissioner has the option to investigate the matter at his discretion.

Please be advised that PSNI replies under Freedom of Information may be released into the public domain via our website @ www.psni.police.uk

Personal details in respect of your request have, where applicable, been removed to protect

confidentiality.