County Durham and Darlington NHS
NHS Foundation Trust

Executive Corridor
Darlington Memorial Hospital
Hollyhurst Road
Darlington
DL3 6HX
Switchboard Tel: 01325 38 0100
Foundation Trust Office: 01325 74 3625
Corporate Records Office: 01325 74 3700

Request for Information Reference: 07.18.16

Direct line: 01325 743700
Email: cdda-tr.cddftfoi@nhs.net

Email only

6 August 2018

**Freedom of Information Act 2000 – Request for Information**

Thank you for your request for information received on 11 July 2018 in relation to the County Durham and Darlington NHS Foundation Trust (Trust). We are dealing with your request under the provisions of the Freedom of Information Act 2000.

You requested information regarding fraudulent email/cyber-attacks. Specifically you asked for:

***I am writing to make a request for information under the Freedom of Information Act 2000.***

Please see answers in red text below.

***1. Q. 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*

***2. Q. 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

***3. Q. 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):*** _____

***4. Q. 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***
- N/A

***If yes, how much was paid:*** _____

***Did the criminals provide the information/program needed to restore systems:***

- ***Yes***
- ***No***
- N/A

***5. Q. 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***

***6. Q. 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***
- N/A

***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:*** _____

***7.Q. 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*

***8.Q. 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:***

- 20 ***from internal workforce***
- _____ ***from third party suppliers***
- _____ ***from both internal and third party suppliers as don't differentiate between senders***
- ***Don't Track***

***9.Q. Do you provide a report button within your email system for end users to report phishing emails?***

- ***Yes***
- No

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

- Yes
- ***No***

***11. Q. Do you have a secure email gateway?***

- Yes
- ***No***
- ***Don't know***

In line with the Information Commissioner's directive on the disclosure of information under the Freedom of Information Act 2000 your request will form part of our disclosure log. Therefore, a version of our response which will protect your anonymity will be posted on the County Durham and Darlington NHS Foundation Trust website.

If you have any queries or wish to discuss the information supplied, please do not hesitate to contact me on the above telephone number or at the above address.

If you are unhappy with the way your request for information has been handled, you can request a review by writing to:

The Chief Executive
County Durham & Darlington NHS Foundation Trust
Darlington Memorial Hospital

Hollyhurst Road
Darlington
DL3 6HX

If, you remain dissatisfied with the handling of your request or complaint, you have a right to appeal to the Information Commissioner at:

The Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Telephone: 0303 123 1113
Website: www.ico.gov.uk.

There is no charge for making an appeal.

Yours sincerely

**Joanna Tyrrell**
**Freedom of Information Officer**