NHS
Surrey and Borders Partnership
NHS Foundation Trust

Information Governance
18 Mole Business Park
Leatherhead
Surrey KT22 7AD

Tel: 01372 216059
Fax: 01372 217114
Email: IGTeam@sabp.nhs.uk

26 July 2018

ID Number – FOI 6022

Title: Fraudulent Emails

I am now in a position to respond to your request; please see our responses below:

Trust Response:

Question	Trust Response
Q. 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.	The Trust do not track this.
Q. 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	Section 31(1)(a) – the prevention or detection of crime of the Freedom of Information Act 2000 (FOIA). We consider this exemption applies, because the release of this information may assist an adversary in carrying out a cyber-attack against us. Section 31(1)(a) is a qualified exemption, and we are therefore required to consider the public interest. The public interest test considered the following: Whilst we acknowledge the public interest in transparency, we are also mindful that there is greater public interest in allowing organisations to operate without threat of attack through the release of information in this manner. Any attack on our IT networks would affect our ability to maintain our services and lead to data breaches.
Q. 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	No

Question	Trust Response
Q. 4 Has your organisation had a device/system infected by ransomware in the last 12 months that was delivered via email: 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: If yes, how much was paid: _____ Did the criminals provide the information/program needed to restore systems:	Never
Q. 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
Q. 6 Are you aware if your organisation/brand has ever been 'spoofed' and used by scammers to send emails trying to trick people If yes, please state how many separate incidents of your organisation/brand being spoofed that you know of:	Yes – but not sure if it was before or after using DMARC
Q. 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? If yes, how many reports have you received in the last 6 months of fake/phishing messages:	No. The Trust do not track how many reports are received.
Q. 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? If yes, how many reports have you received in the last 6 months of fake/phishing messages:	Yes, however the amount of reports received are not tracked by the Trust.
Q. 9 Do you provide a report button within your email system for end users to report phishing emails?	Yes
Q. 10 Does your organisation have a SOC (Security Operations Centre) or IT security team?	Yes
Q. 11 Do you have a secure email gateway?	Yes