St Helens and Knowsley Teaching Hospitals NHS Trust

Ref no:	124160718
From:	Commercial
Date:	16/07/18
Subject:	Most common type of fraudulent email/cyber-attack

REQUEST

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

If this request is too wide or unclear, I would be grateful if you could contact me as I understand that under the Act, you are required to advise and assist requesters. If any of this information is already in the public domain, please can you direct me to it, with page references and URLs if necessary.

I understand that you are required to respond to my request within the 20 working days after you receive this letter.

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

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

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): _____

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

If yes, how much was paid: _____

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

- Yes
- No

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

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

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: _____

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

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:

- _____ from internal workforce

- _____ from third party suppliers

- _____ from both internal and third party suppliers as don't differentiate between senders

- Don't Track

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

- Yes
- No

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

- Yes
- No

Q. Do you have a secure email gateway?

- Yes
- No
- Don't know

RESPONSE

The Trust must do its utmost to protect patient and staff information.

Patient information and staff information are the foundations upon which healthcare is built, and the Trust have a clear responsibility to safeguard this information to ensure we are able to provide the necessary care to our service users.

To provide the requested information above would highlight any vulnerability, should any such vulnerability exist (within hardware or software or architecture or Vendor, etc.), within our IT infrastructure which could be exploited for the purposes of ransomware, other malware, or to withhold/disrupt IT functionality within the Trust.

This information relating to the cyber security agenda is likely to assist criminal offenders thereby seriously threatening the effective delivery of healthcare by the Trust. The act of gathering information as requested, in the hacking arena is known as foot-printing and our network architecture is closely protected to at least NHS protect if not NHS Confidential. Therefore:

Our patients (and staff) must have confidence that their very sensitive personal data will be held securely.

They (patients & staff) must have confidence that we'll be able to provide the services they need.

Therefore, providing the specific requested information would put their confidence at risk.

Furthermore, loss of patient and staff data by such an attack would massively impact upon our ability to provide effective healthcare to our service users.

And therefore, this would be extremely harmful to the public & the services the Trust provides.

Therefore in accordance with Section 31 of the Freedom of Information Act the Trust will not be releasing the requested information as this would prejudice our ability to resist cyber-attacks.